COMNAVRESFOR INSTRUCTION 5510.9A CHANGE TRANSMITTAL 1

From: Commander, Navy Reserve Force

Subj: COMMANDER, NAVY RESERVE FORCE INFORMATION AND PERSONNEL SECURITY MANUAL

Encl: (1) Cover Page and Revised Table of Contents
     (2) Revised Pages 2-10 through 2-13
     (3) Revised Pages 4-3 through 4-7
     (4) Appendix R

1. **Purpose.** To transmit a change to the basic instruction.

2. **Action.** Remove the Table of Contents from the basic instruction and replace with enclosure (1) of this change transmittal. Remove pages 2-10 through 2-12 of the basic instruction and replace with enclosure (2) of this change transmittal. Remove pages 4-3 through 4-7 of the basic instruction and replace with enclosure (3) of this change transmittal. Add enclosure (4), add Appendix R after Appendix Q of the basic instruction.

3. **Records Management.** Records created as a result of this change transmittal, regardless of media or format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

T. W. LUSCHER
Deputy

Releasability and distribution:
This change transmittal is cleared for public release and is available electronically only via Commander, Navy Reserve Force Web site, https://private.navymilitia.navy.mil
DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK VIRGINIA 23551-4615

COMNAVFOR INST 5510.9A
N01S
6 Feb 14

COMNAVFOR INSTRUCTION 5510.9A

From: Commander, Navy Reserve Force

Subj: COMMANDER, NAVY RESERVE FORCE INFORMATION AND PERSONNEL SECURITY MANUAL

Ref: 
(a) SECNAV M-5510.36, Department of the Navy Information Security Program 
(b) SECNAV M-5510.30, Department of the Navy Personnel Security Program 
(c) EKMS 1B 
(d) DoD 5200.01-M, Information Security Program Overview Classification and Declassification, February 2012 
(e) USSAN 1-07, Authorized Classification and Control Marking Register 
(f) National Security Disclosure Policy 
(h) OPNAVINST 5530.14E 
(i) UG-2040-SHR, Users Guide on Controlling Locks, Keys and Access Cards 
(j) DoD Instruction 2000.16 of 2 October 2006 
(k) NDP-1


1. Purpose. To promulgate policies, responsibilities and standards for the administration of the Navy Reserve Force Security Program per references (a) through (k) and enclosure (l). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMNAVFORINST 5510.9.

3. Background. This manual establishes standards for security program management to ensure consistent application of Department of Defense (DoD)/Department of the Navy (DON) Information and Personnel Security Standards.
4. **Scope.** This instruction applies to all personnel, military, civilian and cleared contractors assigned to or employed by any element of Commander, Navy Reserve Force (COMNAVRESFOR). Commands are individually responsible for compliance.

5. **Forms.** The following Forms can be found on the Navy Forms site [https://navalforms.documentservices.dla.mil/web/public/home](https://navalforms.documentservices.dla.mil/web/public/home):
   
   a. SF 312
   b. SF 33
   c. SF 86
   d. SF 700
   e. CFR 2001.80D
   f. OPNAV 5511/14
   g. OPNAV 5511/13

Distribution:
Electronic only, via COMNAVRESFOR Web site
[https://www.navyreserve.navy.mil](https://www.navyreserve.navy.mil)
COMMANDER, NAVY RESERVE FORCE
INFORMATION AND PERSONNEL SECURITY MANUAL
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1</td>
<td>INTRODUCTION AND RESPONSIBILITIES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Background</td>
<td>1-1</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td>1-1</td>
</tr>
<tr>
<td></td>
<td>Discussion</td>
<td>1-1</td>
</tr>
<tr>
<td></td>
<td>Responsibilities</td>
<td>1-2</td>
</tr>
<tr>
<td></td>
<td>Items Not Approved</td>
<td>1-2</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>PROGRAM MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>2-1</td>
</tr>
<tr>
<td></td>
<td>Command Management</td>
<td>2-1</td>
</tr>
<tr>
<td></td>
<td>Documentation</td>
<td>2-1</td>
</tr>
<tr>
<td></td>
<td>Effective Management of Security Programs</td>
<td>2-2</td>
</tr>
<tr>
<td></td>
<td>Duties and Responsibilities</td>
<td>2-3</td>
</tr>
<tr>
<td></td>
<td>Security Manager</td>
<td>2-3</td>
</tr>
<tr>
<td></td>
<td>Assistant Security Manager</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Top Secret Control Officer</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Naval Warfare Publication Library Control Officer</td>
<td>2-7</td>
</tr>
<tr>
<td></td>
<td>North Atlantic Treaty Organization Control Officer</td>
<td>2-7</td>
</tr>
<tr>
<td></td>
<td>Electronic Key Management System Officer</td>
<td>2-7</td>
</tr>
<tr>
<td></td>
<td>Contracting Officer’s Representative</td>
<td>2-7</td>
</tr>
<tr>
<td></td>
<td>Designated Disclosure Authority/Foreign Disclosure Officer</td>
<td>2-7</td>
</tr>
<tr>
<td></td>
<td>Physical Security Officer</td>
<td>2-8</td>
</tr>
<tr>
<td></td>
<td>Trusted Associate Sponsorship Trusted Agent</td>
<td>2-9</td>
</tr>
<tr>
<td></td>
<td>Special Security Officer</td>
<td>2-10</td>
</tr>
<tr>
<td></td>
<td>Senior Intelligence Officer</td>
<td>2-10</td>
</tr>
<tr>
<td></td>
<td>Anti-Terrorism Office</td>
<td>2-10</td>
</tr>
<tr>
<td></td>
<td>Turnover Files/Desktop Procedures</td>
<td>2-11</td>
</tr>
<tr>
<td></td>
<td>Inspections and Inventories</td>
<td>2-11</td>
</tr>
<tr>
<td></td>
<td>Technical Surveillance Countermeasures</td>
<td>2-12</td>
</tr>
<tr>
<td></td>
<td>Emergency Action Plan</td>
<td>2-12</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS (CONT'D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Forms</td>
<td>2-12</td>
</tr>
<tr>
<td></td>
<td>Security Servicing Agreements</td>
<td>2-12</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>SECURITY EDUCATION</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General</td>
<td>3-1</td>
</tr>
<tr>
<td></td>
<td>Responsibilities</td>
<td>3-1</td>
</tr>
<tr>
<td></td>
<td>Types of Briefings</td>
<td>3-2</td>
</tr>
<tr>
<td></td>
<td>Indoctrination/Orientation Briefing</td>
<td>3-2</td>
</tr>
<tr>
<td></td>
<td>Annual Refresher Training</td>
<td>3-2</td>
</tr>
<tr>
<td></td>
<td>Classified Nondisclosure Agreement</td>
<td>3-3</td>
</tr>
<tr>
<td></td>
<td>Security Debriefing</td>
<td>3-3</td>
</tr>
<tr>
<td></td>
<td>Attestation</td>
<td>3-3</td>
</tr>
<tr>
<td></td>
<td>Security Termination Statement</td>
<td>3-3</td>
</tr>
<tr>
<td></td>
<td>Special Briefings</td>
<td>3-4</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>PERSONNEL SECURITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>4-1</td>
</tr>
<tr>
<td></td>
<td>Discussion</td>
<td>4-1</td>
</tr>
<tr>
<td></td>
<td>Command In-processing</td>
<td>4-1</td>
</tr>
<tr>
<td></td>
<td>Personnel Security Investigations</td>
<td>4-2</td>
</tr>
<tr>
<td></td>
<td>Reinvestigations</td>
<td>4-4</td>
</tr>
<tr>
<td></td>
<td>Temporary Access (Interim Clearance)</td>
<td>4-5</td>
</tr>
<tr>
<td></td>
<td>Electronic Key Management System Security Indoctrination</td>
<td>4-5</td>
</tr>
<tr>
<td></td>
<td>Continuous Evaluation</td>
<td>4-5</td>
</tr>
<tr>
<td></td>
<td>Derogatory Information</td>
<td>4-5</td>
</tr>
<tr>
<td></td>
<td>Debrief for Cause</td>
<td>4-6</td>
</tr>
<tr>
<td></td>
<td>Limited Access/Re-Assignment to Non-Sensitive Duties</td>
<td>4-6</td>
</tr>
<tr>
<td></td>
<td>Suspension of Access</td>
<td>4-7</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS (CONT’D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 5</td>
<td>INFORMATION SECURITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Security Program Element Policy</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Information Security Program Data Report (SF-311)</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Self Inspections</td>
<td>5-2</td>
</tr>
<tr>
<td></td>
<td>Security Oversight and Inspection Program</td>
<td>5-2</td>
</tr>
<tr>
<td></td>
<td>Security Assist Visit</td>
<td>5-3</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>CLASSIFICATION AND MARKING</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td>6-1</td>
</tr>
<tr>
<td></td>
<td>Classification Authority</td>
<td>6-1</td>
</tr>
<tr>
<td></td>
<td>New Marking Standard</td>
<td>6-1</td>
</tr>
<tr>
<td></td>
<td>General Guidelines</td>
<td>6-2</td>
</tr>
<tr>
<td></td>
<td>Required Markings on Classified Documents</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Portion Marks</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Mandatory Derivative Marking</td>
<td>6-4</td>
</tr>
<tr>
<td></td>
<td>Classification Challenges</td>
<td>6-5</td>
</tr>
<tr>
<td></td>
<td>North Atlantic Treaty Organization</td>
<td>6-5</td>
</tr>
<tr>
<td></td>
<td>Controlled Unclassified Information</td>
<td>6-6</td>
</tr>
<tr>
<td></td>
<td>For Official Use Only</td>
<td>6-7</td>
</tr>
<tr>
<td></td>
<td>Wikis</td>
<td>6-7</td>
</tr>
<tr>
<td></td>
<td>Instant Messaging, Chat and Chat Rooms</td>
<td>6-7</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>ACCOUNTABILITY AND CONTROL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>7-1</td>
</tr>
<tr>
<td></td>
<td>Accountability and Control</td>
<td>7-1</td>
</tr>
<tr>
<td></td>
<td>Cover Sheets and Classification Labels</td>
<td>7-2</td>
</tr>
<tr>
<td></td>
<td>Reproduction of Classified Material</td>
<td>7-3</td>
</tr>
</tbody>
</table>

Enclosure (1)
## TABLE OF CONTENTS (CONT'D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER 8</strong></td>
<td><strong>STORAGE AND SAFEGUARDING CLASSIFIED MATERIAL</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>8-1</td>
</tr>
<tr>
<td></td>
<td>Responsibilities for Safeguarding</td>
<td>8-1</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td>8-2</td>
</tr>
<tr>
<td></td>
<td>External Markings on Containers</td>
<td>8-1</td>
</tr>
<tr>
<td></td>
<td>Security Container Information SF 700</td>
<td>8-2</td>
</tr>
<tr>
<td></td>
<td>Combinations to Containers, Vaults and Secure Rooms</td>
<td>8-2</td>
</tr>
<tr>
<td></td>
<td>Protecting and Storing Combinations</td>
<td>8-2</td>
</tr>
<tr>
<td></td>
<td>Changing Combinations</td>
<td>8-3</td>
</tr>
<tr>
<td></td>
<td>Key Locks</td>
<td>8-3</td>
</tr>
<tr>
<td></td>
<td>Electrically Actuated Locks</td>
<td>8-4</td>
</tr>
<tr>
<td></td>
<td>Restricted Areas</td>
<td>8-4</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td>8-4</td>
</tr>
<tr>
<td></td>
<td>Care of Workspaces</td>
<td>8-5</td>
</tr>
<tr>
<td></td>
<td>End of Day Security Checks</td>
<td>8-5</td>
</tr>
<tr>
<td></td>
<td>Classified Material Found Unattended</td>
<td>8-6</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Material Storage</td>
<td>8-6</td>
</tr>
<tr>
<td><strong>CHAPTER 9</strong></td>
<td><strong>TRANSMISSION AND TRANSPORTATION</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>9-1</td>
</tr>
<tr>
<td></td>
<td>Hand-carrying of Classified Material</td>
<td>9-1</td>
</tr>
<tr>
<td></td>
<td>Top Secret</td>
<td>9-3</td>
</tr>
<tr>
<td></td>
<td>Secret</td>
<td>9-3</td>
</tr>
<tr>
<td></td>
<td>Confidential</td>
<td>9-4</td>
</tr>
<tr>
<td></td>
<td>Telephone Transmission of Communications Security</td>
<td>9-5</td>
</tr>
<tr>
<td></td>
<td>Material</td>
<td>9-5</td>
</tr>
<tr>
<td></td>
<td>Preparation of Classified Material for Transmittal</td>
<td>9-5</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS (CONT'D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 10</td>
<td>DESTRUCTION OF CLASSIFIED AND SENSITIVE MATERIAL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>10-1</td>
</tr>
<tr>
<td></td>
<td>Destruction Procedures</td>
<td>10-1</td>
</tr>
<tr>
<td></td>
<td>Records of Destruction</td>
<td>10-2</td>
</tr>
<tr>
<td></td>
<td>Methods of Destruction</td>
<td>10-2</td>
</tr>
<tr>
<td></td>
<td>Destruction of Unclassified Material</td>
<td>10-3</td>
</tr>
<tr>
<td></td>
<td>Emergency Destruction</td>
<td>10-3</td>
</tr>
<tr>
<td>CHAPTER 11</td>
<td>CONTROL OF VISITORS AND REQUESTS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>11-1</td>
</tr>
<tr>
<td></td>
<td>Requirement</td>
<td>11-1</td>
</tr>
<tr>
<td></td>
<td>Responsibilities</td>
<td>11-1</td>
</tr>
<tr>
<td>CHAPTER 12</td>
<td>PHYSICAL SECURITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>12-1</td>
</tr>
<tr>
<td></td>
<td>Program Components</td>
<td>12-1</td>
</tr>
<tr>
<td></td>
<td>Sensitive Compartmented Information</td>
<td>12-2</td>
</tr>
<tr>
<td></td>
<td>Facility Documentation</td>
<td>12-2</td>
</tr>
<tr>
<td></td>
<td>Restricted Areas</td>
<td>12-2</td>
</tr>
<tr>
<td></td>
<td>Key and Lock Control Program</td>
<td>12-3</td>
</tr>
<tr>
<td></td>
<td>Foreign Travel</td>
<td>12-3</td>
</tr>
<tr>
<td>CHAPTER 13</td>
<td>INDUSTRIAL SECURITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic Policy</td>
<td>13-1</td>
</tr>
<tr>
<td></td>
<td>Contractor In-processing and Security Files</td>
<td>13-1</td>
</tr>
<tr>
<td></td>
<td>Definitions</td>
<td>13-1</td>
</tr>
<tr>
<td></td>
<td>Form DD-254 Reviews</td>
<td>13-2</td>
</tr>
<tr>
<td></td>
<td>Fleet Forces Command Office</td>
<td>13-2</td>
</tr>
</tbody>
</table>

Enclosure (1)
### TABLE OF CONTENTS (CONT'D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sponsorship</td>
<td>13-3</td>
</tr>
<tr>
<td></td>
<td>Personnel Security Clearance</td>
<td>13-3</td>
</tr>
<tr>
<td></td>
<td><strong>CHAPTER 14</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SECURITY VIOLATIONS AND COMPROMISES</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guidance</td>
<td>14-1</td>
</tr>
<tr>
<td></td>
<td>Reporting and Notifications</td>
<td>14-2</td>
</tr>
<tr>
<td></td>
<td>Documenting Security Violations</td>
<td>14-2</td>
</tr>
<tr>
<td></td>
<td>Security Discrepancies</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Classification of Reports</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Security Incidents Involving Sensitive Compartmented</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Information Technology</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Security Incidents Involving Information Technology</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Security Discrepancies</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Classification of Reports</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Security Incidents Involving Sensitive Compartmented</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Information Technology</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td>Security Incidents Involving Information Technology</td>
<td>14-3</td>
</tr>
<tr>
<td></td>
<td><strong>APPENDIX</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A: Security Manager/Assistant Security Manager Designation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B: Certification of Training and Acknowledgement of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C: Appointment as Top Secret Control Officer Appendix</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D: Appointment as Information Security Officer Appendix</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E: Generic Security Briefing</td>
<td></td>
</tr>
</tbody>
</table>

*Enclosure (1)*
TABLE OF CONTENTS (CONT’D)

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>F:</td>
<td>Indoctrination/Orientation Brief</td>
<td></td>
</tr>
<tr>
<td>G:</td>
<td>Subversion and Espionage Directed Against the United States</td>
<td></td>
</tr>
<tr>
<td>H:</td>
<td>Security Access Eligibility Report</td>
<td></td>
</tr>
<tr>
<td>I:</td>
<td>Reportable Items and Circumstances</td>
<td></td>
</tr>
<tr>
<td>J:</td>
<td>Employee’s outside Employment/Activities</td>
<td></td>
</tr>
<tr>
<td>K:</td>
<td>Personal Attestation Policy</td>
<td></td>
</tr>
<tr>
<td>L:</td>
<td>Sample Access Suspension Notification</td>
<td></td>
</tr>
<tr>
<td>M:</td>
<td>North Atlantic Treaty Organization Security Briefing</td>
<td></td>
</tr>
<tr>
<td>O:</td>
<td>Protection of Hand-Carried Classified Material in a Travel Status Courier Briefing</td>
<td></td>
</tr>
<tr>
<td>P:</td>
<td>Authorization to Hand-Carry Classified Material Onboard</td>
<td></td>
</tr>
<tr>
<td>Q:</td>
<td>Instructions for Couriers</td>
<td></td>
</tr>
<tr>
<td>R:</td>
<td>Sample Letter of Compelling Need for SSBI</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION AND RESPONSIBILITIES

1. Background. References (a) and (b) require all Navy activities to establish and maintain an effective and comprehensive Information and Personnel Security Program (IPSP). IPSP is established to ensure classified information is protected from unauthorized disclosure and granting of access to classified information is clearly consistent with the interest of national security.

2. Policy. COMNAVRESFOR is responsible for the security oversight of all subordinate commands. Commanding Officers (COs) are responsible for compliance, implementation and integrity of DON security programs. The effectiveness of the command's security program depends on the importance given to the program by the CO.

3. Discussion

a. For the purpose of this directive, the term "Classified Material" applies to classified correspondence, messages, publications, working papers and information stored/processed on Information Technology (IT) systems. "Classified Information" pertains to official information that has been determined to require, in the interest of national security, protection against unauthorized disclosure to persons without the proper security clearance and the need to know.

b. North Atlantic Treaty Organization (NATO) marking is not a classification but rather a marking indicating specific procedure for accessing, handling, storage and dissemination. Before having access to accountable treaty information or when access is no longer required, the provisions of reference (c) must be met.

c. Personnel security clearance is the written authority based upon appropriate investigation, which allows an individual access to classified information when they possess the need to know. A person's need to know is based on the necessity for access to, knowledge of or possession of classified information in order to carry out official military or other government duties. Clearance eligibility does not automatically mean access will be provided.
A member's security clearance eligibility and access to classified information will be consistent with the policy to protect such information in the interest of national security and closely monitored in each department. Personnel security access, in excess of mission requirements, will be administratively withdrawn or downgraded.

4. Responsibilities

a. The Force Security Manager (SM) will develop policy, manage and coordinate the IPSP requirements for COMNAVRESFOR. Coordinating program requirements will be executed in collaboration with the following:

(1) Special Assistant for Financial Management for allocation of programming funds.

(2) COMNAVRESFOR Inspector General for command assessment requirements.

(3) Special Assistant for Contracts for administration of industrial security requirements.

(4) Director Anti-terrorism/Force Protection.

(5) Deputy Chief of Staff for Information Technology Program Management.

b. Echelons III, IV and V command COs and Security Managers (SMs) are responsible for the integrity of IPSP requirements within their commands.

5. Items Not Addressed. This order supplements existing information and personnel security directives. It does not fully incorporate all areas of the program. If guidance on a particular matter cannot be found within this instruction or the references, contact COMNAVRESFOR SM.
CHAPTER 2

PROGRAM MANAGEMENT

1. Basic Policy

   a. COMNAVFORSFOR security manager is responsible for the security oversight of all subordinate commands. This manual supplements applicable portions of the references for implementation.

   b. COS and SMs are responsible for implementation and compliance with DON security programs. The effectiveness of the command’s security program depends on the importance given to the program by the CO. COS and SMs are responsible for the integrity of these programs. Security provisions published in amplifying or supplemental instructions within COMNAVFORSFOR will comply with the policies and procedures of higher headquarters directives and this manual.

   c. Echelon III/IV commands are required to send copies of all Security Manager designation letters to Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration (DUSN PPOI).

2. Command Management

   a. Documentation. Command security management required documentation:

      (1) A letter of designation for the Security Manager (SM) from the CO.

      (2) A letter of designation for the Assistant SM (ASM) from the CO.

      (3) A letter of designation for the Special Security Officer (SSO) to administer the command Sensitive Compartmented Information (SCI) security program, if applicable.

      (4) A letter of designation for any Special Security Representatives (SSR).

      (5) Optionally, a letter of designation for the Top Secret Control Officer (TSCO) from the CO to manage and account
for Top Secret materials and Top Secret control assistants (TSCAs) as needed to assist the TSCO. When used, designations shall be in writing.

(6) A letter of designation for the Information Systems Security Officer and Information Assurance Manager (IAM) from the CO.

(7) A letter of designation for the Physical Security Officer (PSO) from CO.

(8) A written command security policy or instruction.

(9) Self inspections.

(10) An Industrial Security Program when the command engages in classified procurement or when cleared contractors operate within areas under the COs control.


(12) Appointment of an Anti-Terrorism Officer (ATO).

b. Effective Management of Security Programs. For an effective program management the Security Manager:

(1) Develops written information and personnel security procedures, including the emergency plan for the protection of classified material.

(2) Formulates and coordinates the security education program within the command.

(3) Ensures compliance with accounting and control requirements for classified material including receipt, distribution, inventory, reproduction and disposition.

(4) Ensures security control of classified visits.

(5) Ensures that all personnel who handle classified sensitive information are appropriately cleared and that request for security investigations are prepared and submitted per reference (b).

(6) Ensures that all investigations and clearances are properly recorded.
(7) In coordination with the department heads and staff assistants, continuously evaluates eligibility for access to classified information as part of the continuous evaluation program.

(8) Coordinates with the command IAM, Financial Coordinator, legal and Drug and Alcohol Programs Advisors on matters of common concern.

3. Duties and Responsibilities

a. SM. The SM is designated in writing and is responsible for the administration of the information, industrial, personnel security and physical security programs either personally or through subordinates. The SM is responsible for promulgating security policies to subordinate commands, implementing policies and procedures for command personnel.

(1) Serves as the principal advisor and direct representative to the commander regarding matters pertaining to personnel security and the classification, security, transmission and destruction of classified information. The SM ensures implementation, supervision and coordination of all activities related to information, personnel security, physical security and foreign disclosure.

(2) Duties may be assigned full-time, part-time or as a collateral duty and must be a military officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the 5 years prior to assignment.

(3) SM will attend the Navy SMs course through either Security Training Assist Assessment Team (STAAT) or Defense Security Service (DSS) within 90 days of appointment.

(4) Understand and validate status of the Reserve Component population.

(5) Track progress and facilitate communication between DOD Central Adjudication Facility and members. Assist personnel with responses to letters of intent and request for information.
(6) Maintains liaison with the Public Affairs Officer (PAO) or Information Security Officer (ISO), as appropriate and the Operations Security (OPSEC) officer to ensure that information, including press releases and photos, proposed or intended for public release, including via website posting, is subject to a security review per reference (d), Volume 2.

(7) Ensures threats to security, compromises and other security violations are reported, recorded and when necessary, investigated.

(8) Ensures that all security violations or incidents involving possible compromise of classified information involving IT systems are investigated and reported. Coordinate after-incident responses involving classified information processed on IT system with the command IAM.

(9) Formulates, coordinates and conducts the activity security education and training program. Organizations with elements that are deployable for contingency operations shall ensure information security training, to include appropriate application to information systems, is an integral part of pre-deployment training and preparation.

(10) Develops security measures and procedures, per reference (d), Volume 3 and other applicable policies, regarding visitors who require access to classified information and facilities containing same.

(11) Develops a written activity security instruction that shall include provisions for safeguarding classified information during emergency situations and military operations, if appropriate.

(12) Coordinates with the command IAM on matters of common concern, as required, for effective management, use and oversight of classified information in electronic form.

(13) Ensures compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

(14) Ensures access to classified information is limited to those with the need to know.

Enclosure (1)
(15) Ensures compliance with the Industrial Security program for classified contracts with the DoD contractors.

(16) Ensures requirements of reference (b) are met when access to classified information is provided to contractors in connection with legitimate government business.

(17) Establishes a viable, ongoing security awareness program. This shall include training program managers, as well as, general awareness training to all-hands. Training shall include the use of the Plan of the Week, bulletin boards and command websites.

(18) Monitors protection system and devices, such as Protective Distribution Systems and Electronic Access Control (EACS) clients to ensure classified material and systems are not compromised, sabotaged or subjected to malicious mischief or other forms of willful interference.

(19) Assists in the development of EAP.

(20) Maintain liaison with the SSO, as appropriate, on issues of common concern.

b. Assistant SM. The ASM duties are to assist the SM in all actions required to carry out the program as described in this manual. The ASM, if assigned, will be either an enlisted person E-6 or above or civilian employee in the Security Administration Series GS-0080 in the pay grade GS-6 or above. The ASM must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI or SSBI-Periodic Reinvestigation (PR) completed within the previous 5 years. The ASM will also attend the Navy SMs course through either the Security Training, Assistance, Assessment Team Atlantic (STAATLANT) or DSS within 90 days of appointment.

c. Top Secret Control Officer. Optional, where circumstances warrant, designate an activity TSCO to manage and account for Top Secret materials and TSCA as needed to assist the TSCO. When used, designations shall be in writing. Top Secret couriers are NOT considered TSCAs. The TSCO must be an enlisted E-7 or above or a civilian employee in the pay grade of GS-7 or above.
(1) An individual designated as the TSCO must have been the subject of a favorably adjudicated, current background investigation and must have Top Secret access. The TSCO shall report directly to the activity SM or the activity SM may serve concurrently as the TSCO.

(2) The TSCO, when designated per paragraph 2.a.(5) of this enclosure, shall:

(a) For paper documents and other physical media (e.g., disk drives and removable computer media), maintain a system of accountability (e.g., registry) to record the receipt, reproduction, transfer, transmission, downgrading, declassification and destruction of Top Secret information, less Security Assistance Program (SAP), SCI and other special types of classified information.

(b) Ensure that inventories of Top Secret information are conducted at least semi-annual (January and July) or more frequently when circumstances warrant.

(c) A joint inventory will be conducted upon appointment and relief of a TSCO. During the inventory each document will be physically sighted.

(d) The relieved TSCO will not be released from the command until all Top Secret accounting discrepancies are resolved to the satisfaction of the new TSCO, SM and the Commander. The new TSCO will then advise the SM of acceptance of the account in writing. The SM will endorse the letter, signifying appointment of the new TSCO and relief of the outgoing TSCO.

d. Naval Warfare Publications Library Control Officer. Optional, where circumstances warrant, a staff officer will be assigned as the Naval Warfare Publications Library (NWPL) Control Officer in writing and guided by the references and this manual. The NWPL Control Officer may not be simultaneously assigned as Electronic Key Management System (EKMS) Officer.

e. NATO Control Officer. Optional, where circumstances warrant, the Commander shall designate a NATO Control Officer and Alternate NATO Control Officer in writing.
f. **EKMS Officer.** A staff member from N6 will be assigned as the EKMS Officer in writing. The EKMS Officer will be guided by references (a) and (c).

g. **Contracting Officer's Representative.** Optional, where circumstances warrant, when assigned, the Contracting Officer's Representative (COR) will be a security specialist, appointed in writing by the Contracting Officer for the purpose of preparing and signing the "Contract Security Classification Specification" (DD Form 254) and revisions thereto and other security related contract correspondence. The COR is responsible to the command SM for coordinating with program managers and technical and procurement officials. The COR will ensure that the industrial security functions are accomplished when Classified Military Information (CMI) or controlled unclassified information is provided to industry for performance on classified or unclassified contracts. The COR will be guided by the provisions of the current edition of reference (a) in writing by one or more qualified security specialists.

h. **Physical Security Officer.** The Physical Security Officer (PSO) serves as the Commander's principal advisor and direct representative in matters pertaining to the physical security of classified information and security of facilities. The PSO ensures implementation, supervision and coordination of all activities related to physical security and alarm systems. The PSO will be designated in writing by the Commander. The PSO will be guided in the performance of duties by reference (h) and this manual.

(1) Coordinate and conduct, in support of the information security program, Physical Security Evaluations of COMNAVRESFOR building/office spaces in establishing or revalidation strong rooms as required for classified information.

(2) Procure security equipment, material and training/education required to control the movement of command personnel/visitors and protect against unauthorized physical access to the command include an Electronic Badge and Access Control Systems, Intrusion Detection System, Key and Lock Control Program and Visitor Control Program.

(3) Manage the Command Key Custodial program and Document Destruction Operations Center.

Enclosure (1)
(4) The incumbent will work with Special Assistants and the Command SM to ensure unique physical security requirements are met in support of the command’s Physical Security and Loss Prevention Program.

i. **Designated Disclosure Authority/Foreign Disclosure Officer.** Optional, where circumstances warrant, the Designated Disclosure Authority (DDA)/Foreign Disclosure Officer (FDO) will be as a minimum a GS-11 or military equivalent and shall be designated in writing.

   (1) The DDA/FDO acts as the clearinghouse for all COMNAVRESFOR Foreign Disclosure related issues. Delegated official authorized to disclose classified information on behalf of COMNAVRESFOR.

   (2) Advise Foreign Disclosure Representative (FDR) who are appointed as the directorate or special staff, point of contact for all foreign disclosure matters within that organization.

   (3) Ensure CMI designated by DoD, requiring protection in the interests of national security and ensures information is limited to the classifications: Top Secret, Secret and Confidential.

   (4) Instruction disclosure in showing or revealing classified information, whether orally, in writing or any other medium, without providing the recipient with a copy of such information for retention. Responsible for ensuring CMI remains under positive U.S. control and material is not physically transferred into the custody of foreign nationals.

   (5) Direct release in providing the recipient of CMI with a copy, in writing or other medium of such information for retention and or ensures physical transfer into the custody of foreign recipient to deter loss of positive control over the material.

   (6) Disclosure Authority official, specifically designated in writing, delegating authority to who may disclose or deny CMI per the provisions of the National Disclosure Policy, provided the information is originated by the official’s department or agency and the official is responsible for the information to be disclosed.

Enclosure (1)
(7) Interact with the international organizations certifying an international body, civilian or military that may have a requirement for receipt of U.S. CMI in carrying out its assigned responsibilities.

(8) Adhere to regulatory guidelines stipulated in reference (k): National Policy and Procedure of CMI to Foreign Governments and international organizations.

(9) Provide security classification guidance on proper security classification and document marking instructions and interact with Controlled Access Program Coordination Office (CAPCO) for the most current marking guidance.

j. Trusted Associate Sponsorship System/Trusted Agent

(1) Optional, where circumstances warrant, the Trusted Agent (TA) shall be designated in writing as COMNAVRESFOR governmental representative and organization TA for the verification of contractors need for a Common Access Card (CAC). Manage the multi-functional "smart" card.

(2) The TA will be the principal and focal entity within the Trusted Associate Sponsorship System (TASS), the focal point for handling contractor accounts and the conduit between the Trusted Agent Security Manger (TASM) and contractors. As such the TA is responsible for vested maintenance of contractor CAC accounts under their charge.

(3) Verify and ensure the appropriate and pertinent data information is included in the web-based TASS for contractors. The incumbent will create contractor accounts in TASS; review and complete contractor application forms, approves returns or rejects the CAC application as applicable. Every 6 months the TA shall re-verify assigned contractors and revoke contractor eligibility for CAC if needed.

(4) Responsible for rejection and/or approval of application. A record will be maintained of all applications and procedures.

(5) The incumbent will verify all (DD 254s) are prepared and on file at all times. Defense Enrollment Eligibility Reporting System must be verified in conjunction with the applicant's request.
(6) Coordinated with Regional TASM who handles the broad geographical region and assignment of the TA within the region.

(7) The TA will also distribute temporary user/password for contractors to gain access to the TASS Web site and complete the applicable form. The contractor CAC issuance is staggered throughout the year so the re-verifying process may be an ongoing task.

k. Special Security Officer

(1) The special security officer (SSO) is the principle advisor on the SCI security program in the command and is responsible to the commanding officer for the management and administration of the program. The SSO is bound by guidelines set forth in reference (a) and (b).

(2) The SM is not responsible for handling or control of SCI.

(3) The SSO will inform the SM on results of SCI access investigations and provide updates on these investigations as they occur.

(4) The SM must advise the SSO of any derogatory information received on an individual in the SCI program.

(5) COMNAVRESFORCOM designates the Commander, Naval Information Force Reserve (COMNAVIFORES FORT WORTH) SSO as the “Force SSO.” The Force SSO, and his subordinate Special Security Representatives, provides support to the entire Navy Reserve.

l. Senior Intelligence Officer

(1) The senior intelligence officer (SIO) is the highest ranking military or civilian individual charged with oversight of the command’s Sensitive Compartmented Information (SCI) security program. COMNAVRESFORCOM designates the COMNAVRESFORCOM (N2), via a letter of designation, as the command SIO.

(2) A primary duty of the COMNAVRESFOR SIO, or “Force SIO”, is to determine Reserve Sailors’ need for access to SCI if they are not in a billet coded for the access. COs who determine one of their Sailors requires this access will request a Letter of Compelling Need, or Compelling Need Statement addressed to the COMNAVRESFOR SIO/COMNAVRESFORCOM (N2). See Appendix R for a sample Letter of Compelling Need.

(3) The Force SIO’s determination of access is based upon an assessment of risk and if a person's services are essential to accomplishing an operation or mission, and demonstrate a clear “need to know.”
(4) The Force SIO will work with supported commands' OSOs and SSOs as necessary to assist those commands in determining SCI access requirements for reserve support, to include documentation in manpower documents where appropriate (i.e., when a billet requires a “Q” functional area code, denoting a position in which the incumbent will require access eligibility to Top Secret Sensitive Compartmental Information material).

4. Anti-Terrorism Officer

a. The Anti-Terrorism Officer (ATO) is responsible for planning, implementation and execution of the commands Anti-Terrorism Force Protection Plan (ATFP).

b. The ATO is responsible for ensuring command personnel are trained annually on Level I Anti-Terrorism training and to ensure all command personnel conducting travel outside of the U.S. receive country specific briefings and other travel requirements as directed by each area of responsibility.

c. The ATO is responsible for implementation of the command’s Random Anti-Terrorism Measures program.

5. Turnover Files/Desktop Procedures

a. Individuals assigned to duties described above will prepare and maintain a turnover file to facilitate the in briefing of personnel assuming those duties. At a minimum such files will contain a copy of this manual, copies of current appointment letters and endorsements thereto, copies of all official correspondence relevant to the position, copies of all custodial documents (inventories, receipts, destruction reports) or a memorandum indicating where the documents may be found and a brief synopsis of the duties of the position.

b. Individuals appointed to positions of responsibility under this manual will prepare and maintain a current desktop procedure folder. This folder will contain detailed instruction for the accomplishment of the duties inherent in these positions.

c. All supervisors will include information pertaining to the supervisory role in their turnover files.

6. Inspections/Inventories

a. In addition to other inspections directed or conducted by higher headquarters, at least once annually, the SM will arrange for a detailed inspection of the Top Secret, Secret, Confidential, NATO, and NWPL accounts.

(1) Evaluations will take place through self-assessments, inspections, oversight visits, and internal reviews. In addition to requirements outlined in the Inspector General Assessment
Guide, Appendix C of reference (a) is a Security Inspection Checklist that should be used as a guide when assessing overall status of a security program.

b. Inspections will review classified management, accountability, and control of classified information. The SM will notify the responsible department head of corrective action required. Results will be reported to the commander with information copies to the staff section concerned. A comprehensive security inspection guide is contained in appendix A.

c. IAM in coordination with the SM, will conduct periodic inspections and evaluations of Information Awareness security procedures throughout COMNAVRESFOR headquarters in conjunction with the semi-annual inventory/inspections.

7. Technical Surveillance Countermeasures. Technical Surveillance Countermeasures (TSCM) surveys and inspections are performed upon request in areas where highly classified information is regularly discussed. Requests for TSCM services will be requested by Intel in writing and will be classified at least Secret. TSCM services will not be requested by telephone, facsimile, or e-mail. Discussions regarding these services will not be conducted in the area to be serviced and will be limited to those personnel with a valid need to know. Guidance for TSCM services is contained in reference (d).

8. Emergency Action Plans. Reference (a) requires each command that handles classified material develop an Emergency Destruction Plan for the protection of classified material in case of natural disaster, civil disturbance, or enemy action. Procedures will be incorporated into the command's Physical Security Plan. Since emergencies of a natural or casualty nature would not normally subject classified material to be captured by enemy forces, securing or removing the material, as directed, should suffice. The primary consideration is the safety and welfare of personnel. EAP consists of augmenting security measures while maintaining safety at all times. Reference (a) appendix 2-B outlines guidelines for developing emergency plans.

9. Forms. Appendix C lists the forms used in the information, personnel, physical, and foreign disclosure security programs.

10. Security Servicing Agreements

   a. Commands may perform specified security functions for other commands via security servicing agreements. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including:

      (1) A command provides security services for another command or the command provides services for a tenant activity.

      (2) A command is located on the premises of another government entity and the host command negotiates an agreement for host to perform security functions.
b. A security servicing agreement will be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement will include requirements for advising COs of any matters that may directly affect the security posture of the command. Append security service agreements to the command security instruction.
CHAPTER 3

SECURITY EDUCATION

1. General. References (a) and (b) require all Echelon III, IV and V commands (except Navy Reserve augmentation units) COs and SMs to establish and maintain an active Security Education program. Program will be tailored to meet the needs of the individual activity and will encompass all personnel regardless of position, rank or grade who are assigned to Echelon III, IV and V commands. The primary purpose is to ensure that all personnel understand the need to protect and safeguard classified information and material. Area Commanders must comply with security education requirements as outlined in references (a), (b) and (d).

2. Responsibilities

   a. Designated Security Officials (i.e. SM, TSCO, PSO) will ensure that activities are provided up-to-date information on security education and course availability.

   b. COs will give special attention to security education programs and ensure they meet the needs of the command.

   c. SMs should have primary responsibility for implementing the security education program and ensuring maximum participation at their commands. The program will be tailored to the command and will consist of the following:

      (1) Security indoctrination for all newly assigned personnel, which stresses the need for safeguarding Classified Information and reporting of threats to national security.

      (2) Orientation of personnel, who will have access to classified information at the time of assignment, regarding command security requirements.

      (3) On-the-job training in specific security requirements for the duties assigned.

      (4) Annual refresher and counter-intelligence briefings for all command personnel.

      (5) Special briefings as circumstances dictate.

      (6) Debriefings upon termination of access.

Enclosure (1)
3. **Types of Briefings**

   a. **Indoctrination/Orientation Briefings.** All personnel, including civilians, military members and on-site support contractors shall receive an initial orientation to the Information Security Program. This initial orientation is intended to:

   (1) Define classified information and Controlled Unclassified information (CUI) and explain the importance of protecting such information.

   (2) Produce a basic understanding of security policies and principles.

   (3) Notify personnel of their responsibilities within the security program and inform them of the administrative, civil and/or criminal sanctions that can be applied when appropriate.

   (4) Provide individuals enough information to ensure the proper protection of classified information and CUI when in their possession. This will include actions to be taken if such information is discovered unsecured; if a security vulnerability is noted or if a person has been seeking unauthorized access to such information. Additional guidance can be found in reference (b) and reference (d), Volume 3.

   b. **Annual Refresher Training**

   (1) At a minimum, all civilians, military members and on-site support contractors with access to classified information shall receive annual refresher training that reinforces the policies, principle and procedures covered in their initial and specialized training.

   (2) Annual Refresher training shall also address threats and the techniques foreign intelligence activities use while attempting to obtain classified information and advise personnel of penalties for engaging in espionage activities and other unauthorized disclosures.

   (3) Refresher training shall also address relevant changes in information security policy or procedures and issues or concerns identified during DoD annual self-inspections.
Information system users shall additionally complete an annual Information Assurance awareness refresher training, per references (b) and reference (d), Volume 3.

(4) Derivative classifiers (i.e., those who create new documents, including e-mails, based on existing classification guidance) shall receive training in derivative classification per references (b) and reference (d), Volume 3.

c. **Classified Nondisclosure Agreement.** All personnel holding a clearance are required to execute a Classified Information Nondisclosure Agreement (SF 312) Appendix F as a condition of access. Execution of this document is only required once in an individual's career.

d. **Security Debriefing.** All personnel who have access to classified information must receive a security debriefing by the SM or ASM under the following conditions:

   (1) Prior to termination of active military service or civilian employment and for a temporary separation of 60 days or more.

   (2) At the conclusion of the access period when a limited access authorization has been granted.

   (3) When a security clearance is revoked for cause.

   (4) When a security clearance is administratively withdrawn.

e. **Attestation.** Every individual who is authorized Top Secret clearance eligibility or who has access to SAP or SCI, will make a verbal attestation confirming that he/she will conform to the conditions and responsibilities imposed by law and regulation on individuals granted such eligibility or access per reference (b), chapter 4.

f. **Security Termination Statement.** The Security Termination Statement (OPNAV 5511/14), Appendix H will be executed by the security office that maintains the individual's clearance information. This termination statement is required when an individual retires, leaves government service or if access is terminated by the command. A copy will be retained for 2 years.
g. Special Briefings

(1) NATO and Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI). Appendix G provides an example of NATO and SIOP-ESI briefings. Briefs should be supplemented by guidance from references (b) and (c) and should include specific job assignments or location requirements.

(2) Foreign Travel. Commanders/COs of Echelon III, IV and V commands must set up procedures per references (a) and (b). Department heads and individual staff members are required to notify the SM or ASM if a staff member, who has access to classified information, plans to travel to or through a high-risk country or attend a meeting in the U.S. or abroad, in which representatives of high-risk countries are expected to participate. The SM or ASM will coordinate the required briefings with AT/FP and NCIS and ensure all requirements are met per the DoD Foreign Clearance Guide. Prior to departure and upon return, member will receive appropriate briefings and debriefings as required. Individuals will execute Foreign Travel Request Form and Foreign Travel Questionnaire. Signed documents will be maintained by the security office.

(3) SCI. Briefings for SCI access will be coordinated by the SM/SSR with the respective servicing SSO office.

(4) Security Awareness Briefings. Security Awareness briefings will be conducted at a minimum of once a year. In the event that world events or current threats require additional security awareness training and/or OPSEC training, each location will provide the additional training and/or security bulletins necessary to all hands and reevaluate current processes related to current risks. The SM will coordinate and direct these briefings, as required.

(5) Counterespionage Briefings. Counterespionage briefings are conducted annually by the local NCIS Field Office for personnel having a Secret or Top Secret clearance. These briefings will be coordinated by the SM.

(6) On-the-Job Security Training. Supervisors are responsible to ensure security practices within the work area are adhered to per references (a) and (b). If additional training is required, the supervisor will arrange for the training to be accomplished with the assistance of the SM.
1. **Basic Policy.** The objective of this chapter is to ensure initial and continued access to classified information and/or initial and continued assignment to sensitive duties for those persons whose loyalty, reliability and trustworthiness are such that entrusting them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security.

2. **Discussion.** Personnel security clearance is the written authority based upon appropriate investigations, which allows an individual access to classified information when they possess the need to know: A person’s need to know is based on the necessity for access to, knowledge of or possession of classified information in order to carry out official military or other government duties. A clearance does not automatically mean that access will be provided. A member’s security clearance and access to classified information will be consistent with the policy to protect such information in the interest of national security and closely monitored in each department. Personnel security clearances, in excess of mission requirements, will be administratively withdrawn or downgraded.

3. **Action.** The Security Manager shall:

   a. Understand and validate status of the Reserve Component population.

      (1) Ensure all Reserve Component personnel are properly reflected in JPAS.

      (2) Submit investigation request for all personnel with missing investigations and investigations greater than 10 years old.

      (3) Determine status of deficiencies for personnel with Revoked or Denied status when investigation is less than 10 years old.

      (4) Submit for reconsideration at Navy Reserve Activity CO discretion.
(5) Track progress and facilitate communication between DOD Central Adjudication Facility and members.

(6) Assist personnel with responses to Letters of Intent and request for information.

(7) Issue NAVPERS 1070/13s as required to document delivery of correspondence.

(8) Enforce timeliness of response expectations.

b. Take appropriate administrative actions based on validated results.

(1) Officers initiate separation for officers w/out clearance eligibility (MPM 1301-227).

(2) Enlisted direct "forced conversion" when current rating requires eligibility. Separate personnel who are unable to convert (MPM 1910-133).

3. Command In-processing

a. Personnel assigned to sensitive duties must receive indoctrination and orientation training on the national security implications of their duties and responsibilities. Each command must develop and maintain a vigorous check-in program for new command members.

b. As a part of the check-in program commands are required to maintain complete and accurate personnel security records per reference (b). Files will contain the following items (as applicable):

(1) Privacy Act Statement on each file.

(2) Copies of Non-Disclosure Agreements/Non-Disclosure Statements and all other indoctrination paperwork.

(3) Copies of Security Access Eligibility Reports (SAER), reports of derogatory information; reports of change in personal status and security violations.

(4) Copies of debriefs (transfers) and Termination Statement (retirement or access suspensions).
4. Personnel Security Investigations

a. Reference (b) outlines requirements for granting access. No individual will be given access to classified information or be assigned sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness based on a completed investigation.

b. In order to provide the appropriate level of background investigation and suitability determination, positions are designated according to potential risk. After determining the position sensitivity level, the appropriate investigation can be requested. Commands should only submit members for investigation that are commensurate with the level of sensitivity of the access required. DoN regulations require personnel in certain fields to maintain continuous eligibility as a requirement of that rating, even when assigned to positions that do not require the same level of clearance. Therefore, personnel assigned to any of the following Information Warfare Community (IWC) career fields will remain eligible as follows:

(1) 1805 Oceanography TS/SCI
(2) 181X Cryptologic Warfare (CW) TS/SCI
   7818 CW Warrant Officer TS/SCI
(3) 182X Information Professional (IP) TS/SCI
   7828 IP Warrant Officer TS/SCI
   682X IP Limited Duty Officer TS/SCI
(4) 183X Intelligence TS/SCI
   683X Intelligence Limited Duty Officer TS/SCI
   7838 Intelligence Warrant Officer TS/SCI
(5) 184X Cyber Warfare Engineer TS/SCI
(6) Aerographer’s Mate TS/SCI
(7) Cryptology Ratings (All) TS/SCI
(8) Intelligence Specialist TS/SCI
(9) Information Technician TS/SCI
c. Commands are required to monitor security investigations through Joint Personnel Adjudication System (JPAS) and initiate investigations as they prepare to expire. The following 2 reports can be used to monitor your command's personnel reinvestigations.

(1) Report 1 – Periodic Reinvestigations:

Step 1: Open JPAS and move to the left hand of the screen click on Reports
Step 2: Click on Periodic Reinvestigations
Step 3: The following should be marked:
   - Report On: Check my office and all subordinates
   - For Persons: Check Own and Serviced
   - Organization: Check all organizations
   - Under Sort: Check Name

(2) Report 2 – Personnel by Eligibility and Access:

Step 1: Open JPAS and move to the left hand of the screen click on Reports
Step 2: Click on Personnel
Step 3: The following should be marked:
   - Report On: Check My office and all subordinates
   - For Persons: Check Own and Serviced
   - Organization: Check all organizations
   - Eligibility: All
   - Investigation: All
   - Position Code: All
   - Sort By: Name

5. Reinvestigations. Security clearance access and eligibility do not expire simply because a PR is overdue as long as individuals have submitted required paperwork for their PR or due to operational factors such as deployment; they are unable to submit required forms in a timely manner. Therefore, commands should not suspend security clearance eligibility or access when justifiable circumstances exist that prevents timely submission of required forms. For example, PRs that become overdue while members are deployed should not result in suspension but should be processed immediately upon their return.

   a. Submit investigations for all personnel with investigations greater than 10 years for Secret eligibility.

   b. Submit investigations for all personnel with investigations greater than 5 years for Top Secret eligibility.

6. Temporary Access (Interim Clearance). Temporary access (also referred to as interim clearance or interim access) may only be authorized by the CO or designee, to individuals
pending completion of full investigative requirements and pending establishment of security clearance eligibility by the Department of the Navy Central Adjudication Facility (DODCAF). Temporary access is a provisional option taken to minimize operational impact. Requirements for temporary access are as follows:

a. Temporary (Interim) TS access requires:
   
   (1) Established Secret or Confidential security clearance eligibility or a current National Agency Check with Local Agency and Credit Checks (NACLC) or Access National Agency Check (ANACI) favorably adjudicated by DODCAF.

   (2) A favorable review of the completed personnel security questionnaire SF-86 revealing no significant eligibility issues as outlined in appendix 10A of reference (b).

   (3) An open submission of the SSBI request to Office of Personnel Management (OPM).

   (4) A favorable review of local records.

b. Interim Secret or Confidential access requires:

   (1) A favorable review of the completed personnel security questionnaire SF-86 revealing no significant eligibility issues as outlined in appendix G of reference (b).

   (2) An open submission of a NACLC (military personnel) or ANACI and Inquiries (civilian personnel) request to OPM.

   (3) A favorable review of local records.

b. Command will record all authorized temporary access in JPAS.

7. **NATO Security Indoctrination.** The accreditation of the Secure Internet Protocol Router Network (SIPRNET) includes the hosting of NATO information. All personnel must receive a NATO security briefing prior to establishing a SIPRNET account per references (b) and (c). Completion of the NATO security briefing shall be documented in one of two ways:

   a. Reporting within JPAS for only those personnel who have a requirement to routinely access NATO information.

   b. Local documentation within the command (e.g., training folder, command database, etc.) for those personnel requiring access to SIPRNET, but do not have a requirement to routinely access NATO information.
c. Access to NATO briefing material is available via the Central U.S. Registry (CUSR) located at the following URL: https://secureweb.hqda.pentagon.mil/cusr/forms.aspx.

8. Continuous Evaluation. The Continuous Evaluation Program (CEP) requires commands to utilize JPAS to report questionable or unfavorable information unmitigated that may be relevant to a security determination. Supervisors and managers play a critical role in assuring the success of CEP. The goal is early detection of an individual’s problems.

a. Derogatory Information. Upon receipt of derogatory information the security official will notify the member’s chain of command. The chain of command will determine based on all facts, whether to suspend or limit an individual’s access to classified information or reassign the individual to non-sensitive duties pending final eligibility determination by DODCAF. If it is determined that sufficient information to suspend access the following actions will occur:

(1) Member is briefed regarding suspension of access locally until issue is resolved.

(2) Issue NAVPERS 1070/13 as required to document delivery of correspondence.

(3) Information documented in JPAS.

(4) Member notified in writing advising them of reason(s) for suspension within 10 working days.

b. Debrief for Cause. DODCAF will have to favorably adjudicate before access can be reinstated. Information is documented in JPAS as an incident and individual is briefed on actions taken regarding incident.

c. Limited Access/Re-Assignment to Non-Sensitive Duties. This is usually performed per a suspension, either local or For Cause.

Note: Administrative withdrawal or downgrading of access is not authorized when prompted by development of derogatory information. In these cases the command must suspend access or debrief for cause. Reports of suspension and/or derogatory information are forwarded to DODCAF with a copy to COMNAVRESFORCOM.

9. Suspension of Access. A request for suspension of access due to derogatory reasons should be an evaluation by the department head and knowledgeable supervisors, in conjunction with an evaluation of the facts by the SM. All requests for suspension of access will be forwarded in a narrative form from the department head/supervisor, to the CO, via the SM, outlining the reasons for the request. All available supporting documentation will be attached as enclosures, i.e., letters of indebtedness, reports of counseling, etc. If the CO elects to suspend the individual's access, the information will be forwarded to DODCAF for a final clearance determination.
a. Per reference (b), when a determination to deny or revoke an individual’s security clearance is initiated by DODCAF, a Letter of Notification (LON) is forwarded by DODCAF to the individual via the CO. Upon receipt, the department head or supervisor and SM will provide a recommendation to the CO to suspend or retain access while the appeal is being processed. Whenever a determination is made to suspend access the following actions will be completed.

   (1) The individual concerned must be notified of determination in writing by the CO or designee, to include a brief statement of reason(s) for suspension action consistent with the interest of national security.

   (2) Commands must report all suspensions to DODCAF no later than 10 working days from the date of suspension action via JPAS, providing sufficient details to support adjudicative review.

   (3) Immediately remove the individual’s access authorization from JPAS, local access rosters and visit certification, and notify all co-workers of suspension.

   (4) Ensure combinations to classified storage containers, vault doors and secure rooms in which individual had access are changed unless sufficient controls exist to prevent access.

   (5) Cancel or hold in abeyance any Permanent Change of Station orders.

b. After completion of the above, SMs will then submit a SAER that contains amplifying information and a command endorsement for continued eligibility/access.

c. The SAER is the opportunity for the command to give all supporting documentation utilizing the whole person concept. Documentation allows DODCAF to make a quick, correct and informed decision regarding the individual’s clearance eligibility. Lack of proper documentation can result in issuance of letter of intent/LON. While not all SAER’s require Non-Judicial Punishment (NJP) actions, NJP actions require submission of SAER to DODCAF to the following address:

    Department of the Navy Central Adjudication Facility
    Building 600 10th Street
    Fort Meade, MD 20755

d. Reestablishing Eligibility after a Denial or Revocation. Following an unfavorable security determination, a request to reestablish eligibility may be submitted after a reasonable passage of time, normally a minimum of 12 months after the concluding unfavorable determination either by Personnel Security Appeals Board, if appeal rights were exercised, or by DON CAF if appeal rights were NOT exercised, provided, the issues which caused the unfavorable determination appear to have been mitigated as outlined by Appendix G, either through the passage of time or other relevant positive developments.
(5) Cancel or hold in abeyance any Permanent Change of Station orders.

b. After completion of the above, SMs will then submit a SAER that contains amplifying information and a command endorsement for continued eligibility/access.

c. The SAER is the opportunity for the command to give all supporting documentation utilizing the whole person concept. ***Please note documentation allows DONCAF to make a quick, correct and informed decision regarding the individual’s clearance eligibility. Lack of proper documentation can result in issuance of Letter of Intent/LON. While not all SAER’s require Non-Judicial Punishment (NJP) actions, NJP actions require submission of SAER to DONCAF to the following address:

Department of the Navy Central Adjudication Facility
Building 600 10th Street
Fort Meade, MD 20755

d. Reestablishing Eligibility after a Denial or Revocation. Following an unfavorable security determination, a request to reestablish eligibility may be submitted after a reasonable passage of time, normally a minimum of 12 months after the concluding unfavorable determination either by Personnel Security Appeals Board, if appeal rights were exercised, or by DON CAF if appeal rights were NOT exercised, provided, the issues which caused the unfavorable determination appear to have been mitigated as outlined by APPENDIX G, either through the passage of time or other relevant positive developments.
CHAPTER 5
INFORMATION SECURITY PROGRAM

1. Information Security Program (ISP) Elements. An interlocking and mutually supporting series of program elements (e.g., need-to-know, investigation, binding contractual obligations on those granted access, security education and awareness and individual responsibility) provides reasonable assurances against compromise of classified information. The foundations of the ISP are the principles of need-to-know and continuous evaluation. The primary security principle in safeguarding classified information is to ensure it is accessible only by those persons with an appropriate clearance, access approval, appropriate access indoctrination and clearly identified need-to-know.

2. Basic Policy. Echelons III, IV and V Commanders (except Navy Reserve augmentation units) are responsible for the effective management of the ISP, per references (b) and (d). The commander or his delegate must establish baseline operating procedures for the ISP. An instruction will cover the operating procedures for all security disciplines at the command, i.e. Personnel, Physical, Information and Industrial. The instruction will also establish procedures to prevent unauthorized persons from accessing classified information, including:

   a. Specific requirements for protecting classified information at command-sponsored meetings and conferences, to include seminars, symposiums, conventions, training activities, workshops or other such gatherings, during which classified information is disseminated.

   b. Procedures to accommodate visits involving access to or disclosure of, classified information.

3. Information Security Program Data Report (SF-311). Conduct random sampling of derivatively classified documents June, July and August to ensure compliance with marking requirements in chapter 6 of references (b) and (d). Commands shall use the SF 311 to document the marking sampling, to ensure consistency throughout the DON.

Enclosure (1)

5-1
a. The requirement to conduct random sampling only applies to commands that have significant classification activity. Significant is defined as 100 or more. Commands with less than 100 are still encouraged to conduct a sampling to assess compliance with marking requirements.

b. Summary of results shall include total number of documents sampled, percentage of each type of discrepancy outlined in enclosure (2) and actions taken to improve marking if there is an error rate of at least 20 percent (Note: this may be covered in items 2 and 3 above).

4. Self Inspections

a. COMNAVRESFOR Echelon III, IV and V commands/activities will establish and maintain an ongoing self-inspection program.

b. Assessment shall be conducted annually following guidelines included in COMNAVRESFOR Command Assessment Guide (Appendix I). An expanded checklist is provided in references (a) and (b). Assessment should reflect implementation portion of the ISP, as well as, overall performance, efficiency and effectiveness of the command’s security program.

c. Discrepancies shall be corrected to ensure compliance with references (a) and (d).

d. Copies of self inspections will be maintained for a period of 3 years.

e. All subordinate commands are discouraged from generating supplemental guidance to the Command Assessment Guide without prior written approval from COMNAVRESFOR.

5. Security Oversight and Inspection Program. Echelon III and IV commands/activities will evaluate and assess the effectiveness and efficiency of the security programs throughout domain.

a. The Security Oversight and Inspection (SO&I) will encompass all of the security disciplines (physical, personnel, information, industrial) to ensure compliance with policy, make sure security programs are cost effective and to ensure the protection of our information and resources from threat of unauthorized disclosure, loss, misuse or damage.
b. Commands will conduct inspection at each subordinate command site every 2 years.

6. **Security Assist Visit.** Program will provide assistance with understanding, identifying and meeting security requirements. Security Assist Visit (SAVs) will also be used to provide security related training to security staff personnel. SAVs can be general in nature or focus on specific areas if known vulnerabilities and/or deficiencies exist. SAVs will be conducted as required and may be scheduled at the request of the CO.
CHAPTER 6

CLASSIFICATION AND MARKING

1. Policy. Information shall be classified only to protect national security. If there is significant doubt about the need to classify information, it shall not be classified. Unnecessary or higher than necessary classification is prohibited by references (b) and (d). Information will be declassified as soon as it no longer qualifies for classification.

2. Classification Authority. COMNAVRESFOR activities have derivative classification authority only. Original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Derivative classification is defined as incorporating, paraphrasing, restating or generating in new form, information that is already classified. Per reference (d), Volume 1, derivative classifiers will:
   
   a. Observe and respect the original classification determinations made by Original Classification Authorities (OCA) and as codified in classified source documents and security classification guides.

   b. Use caution when paraphrasing or restating information extracted from a classified source document to determine whether the classification may have been changed in the process.

   c. Carry forward to any newly created information the pertinent classification markings.

3. New Marking Standard. In order to further facilitate information sharing, improve consistency and enhance operational efficiencies, Echelon III, IV and V commands/activities shall phase-in the marking standard specified by reference (d), Volume 2, over a period of 1 year from the date of issuance.

   a. The marking system specifies a uniform list of authorized security classification and control markings and their authorized abbreviations and portion markings.

   b. Documents marked per previous guidance prior to the end of the transition period (i.e., 1 year after the date of publication of this manual) need not be re-marked with markings
compliant with guidance in this manual. All newly created documents (original and derivative) shall carry compliant markings after the end of the 1-year transition period.

c. New marking standard includes a requirement to add the applicable dissemination control markings to the overall classification line and to portion markings. Primary changes to marking system are:

(1) The overall classification line is referred to as the "banner line."

(2) The applicable dissemination control marking(s) (e.g., Authorization for Release (REL) TO (authorized for release to)) shall be included in the banner line and the portion markings.

(3) The portion marks for subjects and titles shall be placed before the subject or title, as for other text. The previous exception to the placement rules for subjects and titles is no longer authorized.

(4) The standard for annotating dates in the classification authority block is YYYYMMDD. (This format is consistent with the metadata standard; see reference (d), Volume 2, paragraph 2.h.

(5) Markings must appear in the order specified in reference (d), Volume 2, enclosure (4).

4. General Guidelines

a. The proper marking of a classified document is the specific responsibility of the original or derivative classifier (i.e., the author or originator of the information). All classifiers under the purview of COMNAVRESFOR claimancy are designated as "derivative classifiers." Derivative classifiers shall refer to the source document(s), security classification guide(s) or other guidance issued by the OCA when determining the markings to apply.

b. The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text and shall be conspicuous enough to alert anyone handling the document that it is classified.
c. The holder of an improperly marked classified document shall contact the document originator to obtain correct markings and shall apply those marking as required.

5. Required Markings On Classified Documents. All classified documents shall bear the information identified in this section; however, in exceptional cases specific information required by this section may be excluded if it reveals additional classified information. The information is to be shown using these marking elements: banner lines, portion marks component, office of origin, date of origin and classification authority block (OCA or derivative). Specific requirements for each marking element are contained in reference (d), Volume 2. The required information is:

   a. The overall classification of the document (i.e., Confidential, Secret or Top Secret).

   b. Identification of the specific classified information in the document and its level of classification.

   c. Component, office of origin and date of origin.

   d. Identification of the basis for classification of the information contained in the document and of the OCA or derivative classifier.

   e. Declassification instructions and any downgrading instructions that apply.

   f. Identification of special access, dissemination control and handling or safeguarding requirements those apply.

6. Portion Marks. Every classified document shall show, as clearly as is possible, which information in it is classified and at what level. Derivatively classified documents shall be portion marked per their source per reference (d), Volume 2.

   a. Every portion (e.g., subject, title, paragraphs, sections, tabs, attachments, classified signature blocks, bullets, tables and pictures) in every classified document shall be marked to show the highest level of classification that it contains. When deciding whether a sub-portion is to be treated as a portion and separately marked, the criterion shall be whether the marking is necessary to avoid over-classification of
any of the information or to eliminate doubt about the information's classification level. If there are different levels of classification among a portion and any of its sub-portions, then all sub-portions shall be treated as individual portions and marked separately.

b. Portion markings shall be included at the beginning of the respective portion as this position affords maximum visibility to the reader. Thus, the classification level shown always applies to the text immediately to the right of the portion marking.

c. To indicate the appropriate classification level, the symbols (TS) for Top Secret, (S) for Secret and (C) for Confidential shall be used. Portions which do not meet the standards for classification shall be marked with (U) for Unclassified.

7. Mandatory Derivative Markings

a. Derivative classification is the act of incorporating paraphrasing, restating or generating in new form information that is already classified and marking newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents or classification guide issued by an OCA. All classification decisions for COMNAVRESFOR and subordinates will be derivative in nature. When using a classified source document as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document. When using classification guide as the basis for derivative classification, the instructions provided by the guide are to be applied.

b. All classified documents derivatively classified will have the following elements:

(1) Portion Markings,

(2) Overall Classification Markings,

(3) Classification authority block with "classified by" line,

(4) Classification authority block with "derived by" line.
8. **Classification Challenges**

   a. Authorized holders of classified information are encouraged and expected to challenge information that they, in good faith, believe to be improperly classified.

   b. Accomplishing this procedure will start with the command SM where the information originated or the classifier of the information shall be contacted to resolve the issue.

   c. If a formal challenge to classification is appropriate, the challenge shall be submitted via the chain of command, to the OCA of the information with sufficient description of the information (i.e., the classification of the information, its classifier or responsible OCA and reason(s) the information is believed to be improperly classified) to permit identification of the information. The information will be safeguarded at its stated classified level until a final decision is reached.

9. **North Atlantic Treaty Organization.** Marking is not a classification but rather marking indicating specific procedures for accessing, handling, storage and dissemination. Before having access to NATO Information or when access is no longer required, the provisions of reference (d) must be met.

10. **Controlled Unclassified Information.** In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons, per reference (d), Volume 4. Such information is referred to collectively as CUI. Reference (d), Volume 4, identifies the controls and protective measures developed for DoD CUI For Official Use Only (FOUO), Law Enforcement Sensitive, DoD Unclassified Controlled Nuclear Information and limited distribution as well as some of those developed by other Executive Branch agencies.

   a. All unclassified information must be reviewed and approved for release through standard processes before it is provided to the public (including via posting to publicly accessible websites) per reference (d), Volume 4.

   b. **For Official Use Only.** FOUO is a control marking for unclassified information that may be withheld from the public if disclosure would reasonably be expected to cause a foreseeable
harm to an interest protected under the Freedom of Information Act (FOIA). Reference (d), Volume 2 provides guidance regarding appropriate uses of FOUO.

(1) Description. FOUO is a dissemination control applied by the DoD to unclassified information when disclosure to the public of that particular record or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more of FOIA exemptions 2 through 9.

(2) Protection of FOUO Information. During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing or leaving FOUO information unattended where unauthorized personnel are present).

11. Wikis. A wiki is a website that allows users to make changes, contributions or corrections. Wikis may be classified or unclassified; users must be careful not to post classified information on unclassified sites. Refer to reference (d), Volume 2, regarding Wikis requirements.

12. Instant Messaging, Chat and Chat Rooms

   a. Instant messages and chat conversations generally consist of brief textual messages but may also include uniform resource locators, images or graphics.

   b. Information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking and a classification authority block per reference (d), Volume 2.
CHAPTER 7

ACCOUNTABILITY AND CONTROL

1. Overview. All classified information and material must be afforded a level of accountability and control commensurate with its assigned classification. This chapter provides guidance and procedures, in addition to the requirements of reference (a), for accounting and control of classified material received and generated by COMNAVRESFOR commands.

2. Accountability and Control

   a. By definition, certain distinctions exist between the levels of classification (Top Secret, Secret and Confidential) therefore, so does the degree of required accounting and control. Classified materials will be accounted for and controlled as follows:

      (1) TS. Any command holding TS material must:

         (a) Designate, in writing, a TSCO. The TSCO is responsible for receiving, maintaining accountability, distribution and destruction of TS material.

         (b) Ensure that the quantity of TS material is kept to a minimum.

         (c) Provide "cradle-to-grave" accountability. A hand-to-hand continuous chain of receipt is required, even within the command.

         (d) Ensure there is a record of individuals who have had access to TS material - e.g., an OPNAV Form 5511/13 (Record of Disclosure) is maintained for each Top Secret document to identify every individual who has seen or handled the document, including administrative and clerical staff.

         (e) Prohibit the reproduction of TS material without the consent of the originator or higher authority.

         (f) Ensure all records pertaining to the accounting and control of TS material are retained for a minimum of 5 years after the document is transferred, downgraded or destroyed.
(2) Secret. COs shall establish administrative procedures for the control of Secret information appropriate to their local environment, based on an assessment of the threat, the location and mission of their command. These procedures shall be used to protect Secret information from an unauthorized disclosure by access control and compliance with the marking, storage, transmission and destruction requirements of references (b) and (d). Secret and Confidential working papers such as classified notes from a training course or conference, research notes, rough drafts and similar items that contain Secret or Confidential information shall be:

(a) Dated when created.

(b) Conspicuously marked, centered top and bottom of each page with the highest overall classification level of any information contain within, along with the words “Working Paper.”

(c) Protected per the assigned classification level.

(d) Marked in the manner prescribed for a finished document when retained more than 180 days from the date of creation or officially released outside the organization by the originator.

(e) Destroyed, by authorized means, when no longer needed.

(3) Confidential. COs shall establish administrative procedures for the control of Confidential information appropriate to their local environment, based on an assessment of the threat, location and the command’s mission. These procedures shall be used to protect Confidential information from unauthorized disclosure by access control and compliance with the marking, storage, transmission and destruction requirements of references (b) and (d).

3. Cover Sheets and Classification Labels

   a. Classified files, folders and similar groups of documents shall have clear classification markings on the outside of the folder or holder. Attaching the appropriate classified document cover sheet Standard Form (SF) 703, “Top Secret (Cover sheet);” SF 704, “Secret (Cover sheet);” or SF 705
"Confidential (Cover sheet)" to the front of the folder or holder shall satisfy this requirement. These cover sheets need not be attached when the item is in secure storage (e.g., General Services Administration (GSA) approved security container).

b. If not otherwise marked, the SF classification labels listed in subparagraphs (1) through (3) of this paragraph should be used to identify the highest level of classified information stored on IT systems and removable electronic storage media. These labels may also be used on other forms of property to clearly identify the classification level of the information contained in or on that item, when appropriate. In an environment in which both classified and unclassified information is processed or stored, SF 710, "Unclassified (Label)" shall be used to identify unclassified media or equipment. There is no requirement to use SF 710 in environments where no classified information is created or used. If the level of classification of the information on the medium changes (i.e., the information is declassified, downgraded or upgraded), the label shall be replaced or covered by the appropriate label for the new level of classification.

(1) SF 706, "Top Secret (Label)."

(2) SF 707, "Secret (Label)."

(3) SF 708, "Confidential (Label)."

c. Where cover sheets and classification labels are used, the specified SFs must be used unless a waiver is granted.

4. Reproduction of Classified Material. Reproduction is kept to a minimum consistent with mission requirements. All copiers utilized for reproducing classified material will be conspicuously marked with the approved level of reproduction. Areas surrounding reproduction equipment will be checked for classified material that may have been left on nearby desks or thrown in wastebaskets. In the event the equipment malfunctions, system will be checked to ensure that all copies have been removed. Upon completion of reproduction, the equipment will be checked to ensure the original and all copies have been removed. Whenever technology exists in copiers residual data could remain in memory. The IAM will provide operational procedures for clearing each classified copier.
COMNAVRESFORINST 5510.9A
6 Feb 14

CHAPTER 8

STORAGE AND SAFEGUARDING CLASSIFIED MATERIAL

1. Basic Policy. Classified information or material will only be used where there are adequate facilities to prevent unauthorized persons from gaining access. Specific security requirements will depend on the conditions outlined in references (b) and (d). All individuals assigned to COMNAVRESFOR and subordinates are responsible for ensuring classified information and material they prepare, receive, sign for or handle is properly accounted for, stored and safeguarded. Additionally, whenever classified information and material is not in actual use or under surveillance by an authorized individual, it is the responsibility of the custodian to secure the information or material in an approved storage container per references (b) and (d).

2. Responsibilities for Safeguarding

   a. The custodians of classified material must follow procedures to ensure that unauthorized persons do not gain access to classified information by sight or sound or other means. Classified information will not be discussed with or in the presence of unauthorized persons.

   b. Approval to remove classified material will not include permission for overnight storage in any location other than a secure government facility.

3. Storage. Classified material will be stored and locked in GSA approved security containers, strong room or vault that has been certified for the highest level of classification stored in the container. The SM can authorize a work area to be approved for open storage of classified information with proper safeguards in place. Such designations will be written and posted in the area designated as an Open Storage or Secure Room. Reference (a), chapter 7 and 10, provide procedures for storage and safeguarding for TS, Secret and Confidential material. NATO Classified Material will be provided the same storage and safeguards as U.S. Classified Material of equivalent level and may be stored in the same security container but must be physically separated.

4. External Markings on Containers. There shall be no external mark revealing the level of classified information authorized to

Enclosure (1)
be or actually stored in a given container or vault or indicating the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes) or from applying decals or stickers, the Director of National Intelligence requires for containers and equipment used to store or process intelligence information. If a GSA container or vault door recertification is required, such labels and markings must be removed, but may be reapplied as needed after recertification.

5. Security Container Information - SF 700. Maintain a record for each container or vault or secure room door, used for storing classified information. SF 700 with all information blocks completed, shall be used for this purpose. Update the form each time the security container combination is changed.

   a. Part 1 of SF 700 is not classified, but contains Personally Identifiable Information that shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF 700) conspicuously marked “Security Container Information” and stored per SF 700 instructions. If the information must be accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original envelope should be temporarily resealed, to the extent possible, until Part 1 can be placed in a new envelope the next working day.

   b. Part 2 of SF 700, when completed, is classified at the highest level of classification authorized for storage in the security container. It shall be sealed and stored per SF 700 instructions. The classification authority block shall state “Derived From: 32 CFR 2001.800 (3),” with declassification upon change of combination.

6. Combinations to Containers, Vaults and Secure Rooms

   a. Protecting and Storing Combinations. The combination shall be classified at the same level as the highest classification of the material authorized for storage in the container.

      (1) Use SF 700 Part 2 to record the combination and other required data.
(2) If another record of the combination is made, the record shall be marked as required by version 2 of reference (d).

(3) Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers, including vaults and secure rooms.

(4) Security containers, vaults, secure rooms and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(5) A record of the names of persons having knowledge of the combination shall be maintained.

b. Changing Combinations. Only individuals with the responsibility and an appropriate security clearance shall change combinations to security containers, vaults and secure rooms used for storing classified information. Combinations shall be changed:

(1) When the container, vault or secure room door is placed in service.

(2) Whenever an individual knowing the combination to the container or vault door no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

(3) When compromise of the combination is suspected.

(4) When the container, vault or secure room door is taken out of service or is no longer used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50 and combination padlocks shall be reset to the standard combination 10-20-30.

7. Key Locks. Keys and key locks to restricted areas shall be controlled per references (g) and (h). Commercial locks, privately owned locks and the standard Navy brass padlocks are not authorized in restricted areas.

8. Electrically Actuated Locks. Electrically actuated locks (i.e., cipher and magnetic strip card locks) do not provide the degree of protection required for classified information. They
are not to be used as the primary means to safeguard classified material. Classified material must be stored in GSA approved security containers even though the space entry is controlled.

9. Restricted Areas. Only personnel whose duties actually require access and who have been granted appropriate access will be allowed freedom of movement within restricted areas. All others, upon approval, may be granted access to the area but require escorts.

   a. To facilitate the varying degrees of restricted access, control of movement and type of protection required for CMI, the following applies:

      (1) Level Three. An area containing CMI, which is of such a nature that unauthorized access to the area would cause GRAVE DAMAGE to the mission or national security. Only persons whose duties actually require access and who are appropriately indoctrinated with corresponding access are authorized access to space.

      (2) Level Two. An area containing CMI, which is of such a nature that unauthorized access to the area would cause SERIOUS DAMAGE to the mission or national security.

      (3) Level One. An area containing CMI, which is of such a nature that unauthorized access to the area would cause DAMAGE to the mission or national security. This area is designed for the principle purpose of providing administrative control, safety or a buffer area of security restriction for limited or excluded access.

10. Access Control. Restricted areas will be designated in the command security plan and posted with Restricted Area signs per reference (h). Access lists will be posted at entry to Level 2 and 3 areas and will be kept current. If an electronic control system is in use, a computer-generated listing is acceptable. In Level 2 areas, a log of after hour's visitors will be maintained to include Name, Social Security Number, Rate/Rank, time arrived/departed. In Level 3 areas, a log will be maintained as noted above for all visitors.

11. Care Of Workspaces

   a. Echelons III, IV and V commands (except Navy Reserve augmentation units) commanders will ensure adequate security
measures are employed to prevent unauthorized access to classified material, including security measures to prevent persons outside the building and spaces from viewing or overhearing classified material/discussions. The following considerations should be reviewed for areas in which classified information is viewed or discussed:

(1) Ground floor windows or other accessible opening will be equipped with mechanisms to prevent access from the outside.

(2) Windows will be fitted with curtains or blinds and will remain close at all times to prevent visual access.

(3) Sound attenuation for the conference room and other areas where classified discussions occur. TSCM Support is required for conferences involving TS information.

(4) Escorts for contractor maintenance or cleaning personnel requiring access to areas/offices where classified information is stored.

(5) As an added security precaution, under no circumstances will white paper of any type will be disposed in trash cans, implement shred policy.

12. End Of Day Security Checks. COMNAVRESFOR Echelon III, IV and V commands/activities that process or store classified information shall establish a system of security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure. SF 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms and containers used for storing classified material. SF 702, "Security Container Check Sheet," shall be used to record such actions. SFs 701 and 702 shall be retained and disposed of as required by records destruction management schedules. Personnel conducting security checks will make sure that:

a. All classified material is properly secured.

b. Burn bags are properly stored.
c. Classified shorthand notes, post-it-notes, rough drafts and similar working papers have been properly stored or destroyed.

13. Classified Material Found Unattended. Any classified material found unattended or not properly stored must be secured immediately. Notify the SM if any material is found unattended during normal working hours. After working hours, any security discrepancies must be reported to the Command Duty Officer (CDO), if applicable. If a safe is discovered open after hours in an unsecure space, the person finding the open security container will maintain a guard on the container until the CDO is contacted. The CDO will assess the situation and call the custodian to report to work to conduct an inventory of the safe's contents. The SM will be notified the next working day or earlier if assistance is required. Procedures outlined in references (b) and (d) will be adhered to in documenting security violations.

14. Unauthorized Material Storage. Valuables, such as money, jewels, precious metals, narcotics, privately owned material, etc., will not be stored in the same containers used to store and safeguard classified material.
CHAPTER 9

TRANSMISSION AND TRANSPORTATION

1. Basic Policy. Transmission of classified material is the movement of classified information or material from one place to another. Transmission of classified material by commercial aircraft must be approved by the SM. Area Commanders have the authority to approve escorting or hand carrying of classified material on commercial passenger aircraft. The following policies apply to the movement of classified material:

   a. Unless otherwise restricted, movement can either be by car, bus, train, ship and plane or electronically through computers.

   b. Movement of classified material across national borders is not permitted unless arrangements have been made to prevent inspections by customs and the postal service.

   c. Foreign carriers may not be used to transport classified material unless the U.S. escort has physical control of the material.

2. Hand-carrying of Classified Material. The hand-carrying of classified material must occur when the material is urgently needed for a specific official purpose, there is a specific reason that the material cannot be transmitted by other approved means to the destination within sufficient time for the purpose and when it is mission essential. When classified material will be hand carried, personnel must comply with the following procedures.

   a. Individuals must be designated, in writing, as a courier by the SM or ASM.

   b. Individuals must be courier briefed and a record maintained indicating a briefing was provided and subject understands the procedures.

   c. Complete a DD 2501 (courier card) provided by the Security Office for hand carrying of classified material.

(1) Only the last four (4) of the individual’s social security number shall be used in completing the DD Form 2501.

Enclosure (1)
(2) The use of the DD Form 2501 for verification of authorization to hand-carry SCI or SAP information shall be according to policies and procedures established by the official having security responsibility for such information or programs.

d. Individual hand-carrying classified material within the confines of the command will use the appropriate cover sheet, SF 704, 705 or 706, as applicable, to protect against casual observation during transit.

e. If hand-carrying classified material on commercial aircraft, a courier letter is required along with courier card. The letter must indicate full name of courier, agency, type of identification the individual will present, description of material being carried, (example, 3 sealed packages, 9" x 8" x 24"), addressee and sender; place of departure, destination (transfer points), date of issue and expiration date of letter not to exceed 7 days from date of issue).

f. The courier letter must include the name, title and signature of the official issuing the letter.

g. The SM will provide sequentially numbered Courier Authorization Cards, DD Form 2501, for use by personnel who will be hand-carrying classified material. The DD Form 2501 will be issued to an individual and will expire 2 years from date of issue. Prior to issuance of a DD 2501, a "Protection of Classified Material During Hand-carrying in a Travel Status Briefing" must be executed.

h. The inner wrapping will be stamped with the classification of the material contained therein. If the classified material is to be transferred to the command/activity that it is being hand-carried to, the requirements per reference (a), chapter 9, are as follows:

<table>
<thead>
<tr>
<th>HAND-CARRYING REQUIREMENTS</th>
<th>LOCAL AREA (AUTO/WALKING)</th>
<th>GOVT AIR</th>
<th>COMM AIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Briefing</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Courier Card</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Double-Wrapped</td>
<td>X*</td>
<td>X*</td>
<td>X</td>
</tr>
</tbody>
</table>

Enclosure (1)
Locked Briefcase | X | X | X
---|---|---|---
Authorization Ltr | X | X | X
Protected | X | X | X

*Outer wrapper may be locked briefcase.

3. **Top Secret.** TS material will be transmitted by:
   
   a. The Defense Courier Service.
   
   b. The Department of State Courier System.
   
   c. Cleared and designated U.S. military personnel, government civilian employees or DoD contractors traveling on a conveyance owned, controlled or chartered by the government.
   
   d. Cleared and designated U.S. military personnel or government civilian employees by surface transportation.
   
   e. Cleared and designated U.S. military personnel and government civilian employees on scheduled commercial passenger aircraft on flights outside the U.S. For transmission of classified material, area commanders have the authority to approve the transmission of classified material.

4. **Secret.** Secret material will be transmitted by:
   
   a. Defense Courier Service when U.S. control of the material cannot be maintained. (This does not apply to SCI and Communications Security (COMSEC) material).
   
   b. The Department of State Courier System via registered mail to the State Department Pouch Room.
   
   c. Appropriately cleared contractor employees within and between the U.S. and its territories when employees have the classified information under constant custody/protection at all times.
   
   d. U.S. Postal Service registered mail within and between the U.S. and Territories.

Enclosure (1)
e. U.S. Postal Service registered mail through Army, Navy or Air Force Postal Service facilities outside the area per reference (a), chapter 9.

f. Reference (a) outlines the restrictions for qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the DoD Industrial Security Program.

g. Federal Express or the current holder of the GSA contract for overnight delivery when approved by the official command mail control officer. The following restrictions apply to the transmission of classified material:

(1) Use of service is on an exception basis, when applicable postal regulations are met.

(2) An urgent requirement for overnight delivery for the executive branch to a DoD component or a cleared DoD contractor facility within the U.S. and its territories.

(3) The delivery service shall be U.S. owned and operated, provide automated in-transit tracking to ensure package integrity during transit.

(4) Sender shall ensure that an authorized person is available to receive the delivery and shall verify the correct address.

(5) Under no circumstances shall the release signature block on the receipt label be executed.

(6) The use of external (street-side) collection boxes is prohibited.

5. Confidential. Confidential material will be transmitted in one of the following manners.

a. U.S. postal service registered mail will be used:

(1) For NATO confidential.

(2) For mail to and from Fleet Post Office and Army Post Office addressees located outside the U.S. and its territories.
(3) To other addressees when the originator is uncertain that their location is within the United States.

6. Telephone Transmission of Classified Material. Classified material will not be transmitted over the telephone except on approved Secure Terminal Equipment.

7. Preparation of Classified Material for Transmission. Classified material, which is to be transmitted, will be properly wrapped. Area commanders must designate personnel to ensure compliance with reference (b).

   a. Secret material will be prepared for transmission in a manner as to protect from unauthorized disclosure. When mailing classified material, it will:

      (1) Be double wrapped and will be enclosed in two opaque, sealed envelopes or similar wrappings.

      (2) Be addressed to an official government activity or DoD contractor. (Contractor facility clearance must be verified by the MSC Security Office prior to transmission). Never address to an individual.

      (3) Show complete and correct address on inner envelope. Consult Navy Standard Distribution List (SNDL) to verify mailing address.

   b. If hand-carried, a locked briefcase will serve as the outer wrapper or cover. During shipment of classified material, under no circumstances will the material or package be left unattended in a closed or locked compartment of a vehicle or at a hotel overnight. Material must be delivered, without making any stops (including at a hotel or home), to the nearest military installation for storage.

8. Transmission of Communications Security Material. Communications Security (COMSEC) material will be transmitted per reference (c) and reference (d), Volume 3. Material will only be transmitted through COMSEC.

   a. Area commanders must comply with authorized security procedures in place.

   b. Classified information will not be discussed or transmitted over the telephone except on STE phones. Talking around a subject is "prohibited."

Enclosure (1)
DESTRUCTION OF CLASSIFIED AND SENSITIVE MATERIAL

1. Basic Policy. Classified material shall be destroyed when there is no longer a requirement for maintaining the material. Echelons III, IV and V Commanders (except Navy Reserve augmentation units) are responsible for the disposal of unnecessary classified material holdings. This does not apply to COMSEC material where there are additional security procedures.

2. Destruction Procedures. Local Standard Operating Procedures will outline specific instructions regarding destruction of all classified material. Destruction may be recorded on OPNAV Form 5511/12 Classified Material Destruction Appendix P or on any other record which includes complete identification of the material, number of copies destroyed and the date of destruction (e.g., command route sheet). Witnessing officials must be cleared for highest classification being destroyed and at least one of the two witnesses must be an E5/GS-5 equivalent or above. Officials destroying top secret material must be the TSCO or TSCA.

   a. Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding and physical destruction of components or media.

   b. Documents and other material identified for destruction shall continue to be protected as appropriate for their classification until actually destroyed.

   c. Commanders of Echelons III, IV and V commands (except Navy Reserve augmentation units) with classified holdings shall establish at least one day each year when specific attention and effort is focused on disposing of unneeded classified material (clean-out day).

3. Records of Destruction

   a. Top Secret Messages and Correspondence. The TSCO is responsible for recording and maintaining all records of
destruction for top secret material. These records will be maintained for a period of 5 years from date of destruction.

b. **Secret Messages.** Per reference (a), records of destruction are not required for secret messages processed by the message centers. In addition, messages received by the command for action/information (except for NATO and special access) do not require a record of destruction providing two individuals are present during the entire destruction process.

c. **Secret Material (correspondence, plans, etc.).** A record of destruction is no longer required unless there is a routing sheet attached to the correspondence. If the document has been placed in classified inventory, destruction information must be provided to Command Classified Mail and File Clerk.

d. **Confidential/Sensitive/FOUO.** Confidential, sensitive and FOUO material will be destroyed by authorized means and does not require a record of destruction.

e. **Burn bags.** Each burn bag will be protected by the measures required for the highest level of classification they contain. Burn bags ready for destruction are to be stored in one location and safeguarded accordingly. In spaces not operational 24-hours per day, burn bags will be secured in a locked security container, vault or other authorized storage as outlined in reference (a), chapter 10, when an office is vacated for any reason. Top Secret will be processed through the TSCO not routinely placed in burn bags. The destruction witnesses will sign the register when destroyed and retained by the Command SM/Officer for a period of 2 years.

4. **Methods of Destruction**

a. Effective 1 January 2011, only equipment listed on an Evaluated Products List (EPL) issued by National Security Agency may be used to destroy classified information using any method covered by an EPL. EPLs currently exist for paper shredders, punched tape destruction devices, optical media destruction devices for compact discs and digital video discs, degaussers (for magnetic media sanitization) and disintegrators (for paper and punched tape material). The EPLs may be obtained by calling (410) 854-6358 or at: [http://www.nsa.gov/ia/guidance/media destruction guidance/index.shtml](http://www.nsa.gov/ia/guidance/media destruction guidance/index.shtml).
b. **Declassifying or Clearing of Magnetic and Non-Magnetic Storage Media.** Classified IT storage media (e.g., hard drives) cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal. Advances in technology continue to provide challenges as well as ways to retrieve deleted information. Personnel should be advised that retrieval of information using laboratory methods is a threat, therefore, when in doubt seek guidance from command IAM for proper method for destruction of media.

5. **Destruction of Unclassified Material.** Unclassified material, classified material that has been downgraded to unclassified, FOUO material and unclassified messages should be handled with care and efforts made to protect sensitive information from public access. Implementing official unclassified basic destruction procedures is advised and encouraged. Marking burn bags with FOUO and using for official information decreases possible disclosure of official information to public and adversary.

6. **Emergency Destruction.** Reference (a), Appendix B, sets guidelines for procedures needed for emergency destruction. Instructions for destruction of COMSEC material are outlined in reference (c).
CHAPTER 11

CONTROL OF VISITORS AND REQUESTS

1. Basic Policy

   a. Commanders will establish a visitor access program that will document visits involving access to or disclosure of classified information. As a minimum, these procedures shall include verifying the identity, personnel security clearance, access (if appropriate) and need to know for all visitors. Policy should also outline escorted and unescorted access to command facilities.

   b. JPAS is the system of record for all DoD access determinations and clearance verification. Scattered Castles shall be utilized to validate Intelligence Community member’s security clearance access. **Note: Visit requests are not required for the SCI community - only JPAS or Scattered Castles validation.

2. Requirement

   a. Visit requests shall be processed and security clearance and access level verified using JPAS for DoD civilian, military and contractor personnel whose access level and affiliation are reflected in JPAS. Fax, telephone or other contact method shall only be utilized for those personnel whose access level and affiliation are not reflected in JPAS.

   b. Visits by foreign nationals, except for activities or events that are open to the public, shall be handled per reference (b) and documented in the Foreign Visits System Confirmation Module.

3. Responsibilities

   a. Ensure access to classified material during a classified visit is based on need to know and only then, after identification and security clearance have been verified.

   b. Provide escort as required. Movement of all visitors shall be restricted, as may be necessary to protect classified information.

Enclosure (1)
As a matter of convenience and courtesy, flag officers and their civilian equivalents shall not be required to sign visitor records or display identification badges when being escorted as visitors.

c. Ensure that a department/division activity Visitor Control Log is maintained for restricted areas per references (a) through (c). Visitor control logs will be held for a minimum of 2 years after the date of the latest entry.
CHAPTER 12

PHYSICAL SECURITY

1. Basic Policy. The Physical Security Program is security concerned with active and passive measures designated to prevent unauthorized access to personnel, equipment, installations and information, to safeguard them against espionage, sabotage, terrorism, damage and criminal activity.

2. Program Components

   a. A robust physical security program employs physical protective and security procedural measures in combination with active and/or passive systems, technologies, devices and security personnel which are used to protect assets from possible threat. Commands will employ complimentary security controls sufficient to deter, detect and delay.

   b. Command physical security programs will include the following components as applicable:

      (1) Accredited/Designated Facilities Documentation. All pertinent accreditation for Sensitive Compartmented Information Facilities/or Designation information for Secure Rooms, Controlled/Restricted Access Areas will be updated annually.

         (a) SCI Facilities.

         (b) Secure Room/Vault.

         (c) Controlled Access Area.

         (d) Restricted Access Area.

         (e) Restricted Areas (Level One, Level Two, Level Three).

      (2) AT Plan.

      (3) Random Anti-Terrorism Measures Program.

      (4) Key and Lock Control Program.

      (5) Level I Anti-Terrorism Training.

(7) Visitor Control Procedures.

(8) Travel Awareness Briefings.

c. Security Officials with facilities, buildings and/or rooms which do not meet required standards will use the Unfunded Request to notify COMNAVRESFORCOM Security. A mitigation plan that identifies measures that will be implemented until funding is available to correct deficiency is required.

d. Security Officials will submit requests for waivers/exceptions to COMNAVRESFORCOM (N0IS).

3. Sensitive Compartmented Information Facility Documentation

a. Construction Security Plan is required for all facility modifications and/or changes to the secure area (new penetrations, replacing doors, removing walls, etc.).

b. Statement of Work (SOW) is required for all modifications/upgrades.

c. Concept of Operations required for new construction.

d. Updated Fixed Facility Checklists required for all modifications/upgrades.

e. Updated TEMPEST Addendum (as applicable).

f. Facility/building drawings.

4. Restricted Areas

a. Restricted areas shall be established in writing by the CO within his or her jurisdiction per reference (b) and section 797 of title 50, U.S.C. Designated restricted areas shall be a part of installation plans or local instructions for physical security.

b. C0s shall publish a consolidated list of all restricted areas and mission essential/vulnerable areas not designated as restricted areas aboard the installation, including tenant command restricted areas.

Enclosure (1)
This list shall be contained in the installation plan, shall be reviewed annually and shall specify which areas are vital to national security. This list should be limited to official use only.

c. Tenant COs shall publish and inform the Officer in Charge and region commander, in writing, of all areas under their control that are designated as restricted areas. Particular attention will be paid to those areas that are vital to national security.

d. COs shall establish restricted areas around assets and facilities to protect mission-critical or sensitive assets or programs, security interests, classified material, nuclear material, conventional Arms, Ammunition and Explosive (AA&E), biological select agents and toxins, drugs, precious metals or precious metal-bearing articles, articles or funds having high likelihood of theft and certain unclassified chemicals.

5. Key and Lock Control Program

a. Commanders and COs shall designate a Key Control Custodian and establish a key and lock control program for all keys, locks, padlocks and locking devices used to meet security and loss-prevention objectives of this instruction. This requirement does not include keys, locks and padlocks used for convenience, privacy, administrative or personal use.

   (1) The Key Control Custodian will maintain the command’s overall key and lock control program outlined in reference (h). Keys to command Restricted Areas are maintained in locked key cabinets and security containers based on level of classification for space.

   (2) Key Control Custodian is required to perform spot checks and inventory all keys at least quarterly.

b. Security requirements for sensitive locks and keys used to provide security of AA&E are covered in reference (h).

6. Foreign Travel

a. Procedures will be established for coordinating OCONUS AT/FP travel requirements to include foreign travel briefings, documentation of foreign travel and development of Individual Force Protection Plans for all command members.
b. Commands with facility and/or building responsibilities will ensure an ATO is appointed in writing and has received appropriate training for the execution of duties.

c. Security Officials will ensure a foreign travel briefing is provided to all personnel who are traveling, either officially or unofficially, to foreign countries.
CHAPTER 13

INDUSTRIAL SECURITY

1. Basic Policy. Commanding Officer shall establish an Industrial Security Program if their command engages in classified procurement from industry both from the prime and sub levels. However, a requirement to conduct an investigation may still exist dependent upon the national security significance of the area or sensitivity of the information involved. Command security procedures shall include appropriate guidance, consistent with DoD and DON policy manuals.

2. Contractor In-processing and Security Files. Commands must maintain security files for all contracts. Files will contain all indoctrination/orientation documentation provided to military and civilian personnel. In addition, if the contractor is working on a classified contract, a copy of current Contract Security Classification Specification Document DD 254 (SOW) is also required for retention in the file.

   a. Federal Acquisition Regulation requires the Form DD-254 be incorporated in each classified contract.

   b. The Form DD 254 provides the contractor (or subcontractor) the security requirements and the classification guidance necessary to perform on a classified contract.

   c. The form is only valid if signed by government representative.

3. Definitions

   a. CSO - Cognizant Security Office.

   b. DISCO - Defense Industrial Security Clearance.

   c. DSS - Defense Security Service.

   d. FCL - Facility Security Clearance.

   e. FSO - Facility Security Officer.

   f. GCA - Government Contracting Agency.

   g. JPAS - Joint Personnel Adjudicative System.

Enclosure (1)
4. **Form DD-254 Reviews**

   a. Security personnel will review the Form DD-254 of each contractor assigned to them to validate security requirements listed for the contractor.

   b. The government provides security requirements and guidance to prime contractors for classified contracts primarily by incorporating a DD Form 254 into every contract. The DD 254 forms tells the contractor what items need to be protected and to what degree.

   c. Contractors must have COR assigned to them. CORs are the only authorized individuals to nominate a contractor for access to SCI. This means an individual who is designated and authorized in writing by the contracting officer to perform specific technical or administrative functions on contracts or orders. The term COR includes any individual (military or civilian) performing these types of functions on contracts regardless of the term used to describe their position or assignment (e.g., alternate CORs, Contracting Officers’ Technical Representative, task order monitor, etc.). These individuals serve a critical role in assuring contractors meet the performance requirements of contract terms of cost, quality, quantity and schedule.

5. **Facility Clearance (FCL) Office**

   a. FCL. DSS Facility Clearance Branch makes the administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category. The facility must meet several eligibility requirements, as described in reference (b).

   b. **Verification.** To verify a FCL for an organization, the Information Security Officer (ISO) will request an account from DSS and log into the Industrial Security Facilities Database (ISFD) at: [https://isfd.dss.mil/ISFDweb/](https://isfd.dss.mil/ISFDweb/).
(1) The SM is responsible for submitting the Commercial and Government Entity Code from all completed DD 254 into ISFD.

(2) The verification is valid for a period of 3 years. During that period, notification will be sent from DSS of any changes in FCL to the ISO.

6. Sponsorship. If a contract requires the sharing of classified information during the acquisition cycle, N43/N00CT Contracting, in coordination with the technical requirements code, will work with the SM to prepare a request for Defense Industrial Security Clearance Office to initiate facility clearance action. The request must include:

   a. Facility to be cleared.

   b. Details of classified acquisition need requiring the clearance action.

   c. Level of clearance.

   d. Any storage requirements.

7. Personnel Security Clearance

   a. Access. Access is the ability and opportunity to obtain knowledge or possession of classified information. The dissemination of classified information orally, in writing or by other means shall be limited to those persons whose official duties require knowledge of that information. An individual will not have access to classified information simply because of the level of his or her security clearance. No individual shall be granted access to classified information solely by virtue of rank or position. Access is granted only on a need-to-know basis.


8. Reporting. All personnel are required to notify their supervisor or command security manager when they become aware of information with potentially serious security significance.
regarding someone with access to classified information or assigned to sensitive duties; in accordance with APPENDIX G of reference (b) as listed below. The criteria apply to anyone who holds a clearance (military, civilian or contractor) per references (a) and (b).

a. Allegiance to the United States,
b. Foreign influence,
c. Foreign preference,
d. Sexual behavior,
e. Personal conduct,
f. Financial considerations,
g. Alcohol consumption,
h. Drug involvement,
i. Emotional, mental and personality disorders,
j. Criminal conduct,
k. Security violations,
l. Outside activities and
m. Misuse of Information Technology
CHAPTER 14

SECURITY VIOLATIONS AND COMPROMISES

1. Guidance. Reference (a) and reference (d), Volume 3, outline procedures for reporting security violations and compromises. This reporting is valuable in accessing if security procedures need attention or if security training may be needed. It is of the utmost importance that personnel promptly report security violations to determine cause and decrease violation reoccurrence. The following definitions apply:

a. Infraction. An infraction is a security incident involving failure to comply with requirements (i.e., the provisions of references (b) and (d), this manual or other applicable security policy) which cannot reasonably be expected to and does not, result in the loss, suspected compromise or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

b. Violation. Violations are security incidents that indicate knowing, willful and negligent for security regulations and result in or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

(1) Compromise. A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access or a need to know).

(2) Loss. A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).

c. Inquiry. An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had or could have had access to the information.
The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken and makes recommendations as to the need for further corrective action or a more in-depth investigation.

2. Reporting and Notifications

   a. Persons having knowledge of the possible loss, compromise or unauthorized disclosure of classified information or other violation of security shall immediately report this information to the chain of command. COs, Officer's-in-Charge and local department heads will notify the SM.

   b. If the person believes the Commander or the SM may have been involved in or responsible for the incident, he or she may report incident directly to COMNAVRESFOR Security (NOIS).

      (1) A preliminary Inquiry Officer shall be assigned to document facts and determine if a compromise or possible compromise occurred.

      (2) NCIS local office will be notified by the Commander or SM (Note date and agent notified to include in the preliminary inquiry). Per reference (a), preliminary inquiries will be completed within 72 hours of initial notification of the violation. The procedures for conducting a preliminary inquiry are outlined in reference (a), Chapter 12. Security violations involving a possible national security case will be processed per reference (a) and reference (d), chapter 12 and Volume 3.

3. Documenting Security Violations. All security violations will be documented. Preliminary inquiries which determine that no compromise or damage to national security occurred will be forwarded to COMNAVRESFOR via appropriate chain of command. If a preliminary inquiry indicates that there is a possible compromise; however, there are no security weaknesses, damage to national security can be assessed as minimal and no disciplinary action is contemplated, the report will be sent to the immediate superior in command. (Note: possible compromises involving Secret or Top Secret material cannot be assessed as minimal damage to National Security until a more thorough investigation is conducted).
4. **Security Discrepancies.** A security discrepancy is an administrative or clerical error involving classification markings and/or downgrading or declassification instructions. A Security Discrepancy Notice (OPNAV 5511/51) will be sent to the sender when classified material is received by the command that is improperly mailed, marked or packaged.

5. **Classification of Reports.** Security incident reports shall be classified according to the content of the report and at the level prescribed by the applicable program security classification guides. At a minimum, reports shall be designated FOUO and marked as required by reference (d) Volume 4, in order to provide appropriate protection for information regarding personnel involved and information that could facilitate unauthorized access to classified information. If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting or loss in a foreign country), the report and location of the compromise (e.g., geographic location of unrecoverable equipment) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure.

6. **Security Incidents Involving SCI.** Actual or potential compromises involving SCI shall be reported to the activity SSO and handled per reference (i).

7. **Security Incidents involving IT.** Actual or potential compromises of classified information involving IT, automated information systems or computer systems, terminals or equipment shall be reported, per reference (a) and reference (d), Volume 3, through appropriate channels by IAM to the organization SM.
APPENDIX A

Security Manager (SM)/Assistant Security Manager (ASM)
Designation Letter

From: Command/Organization Name
To: (Rank, Name of Appointee)

Subj: APPOINTMENT AS COMMAND SECURITY MANAGER/ASSISTANT SECURITY MANAGER

Ref: (a) SECNAV M-5510.36, Department of the Navy Information Security Program
(b) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(c) COMNAVRESFORINST 5510.9(Series)

1. You are directed to familiarize yourself with duties and responsibilities, per references (a) through (c). You will assess the status of the program and provide a written report detailing any deficiencies. You will ensure all aspects of the program are coordinated with the appropriate individuals and that all command personnel are kept abreast of changes in policies and procedures and provided assistance in solving security related problems.

2. You are hereby designated as the "Command Security Manager" and will familiarize yourself with the requirements of references (a) and (b).

3. This appointment supersedes all previous appointments.

Signature

Copy to:
Echelon III SM
Echelon IV SM

Enclosure (1)
APPENDIX B

Certification of Training and Acknowledgement of Responsibilities

From: (Name, Rate/Rank/Grade)
To: Commanding Officer

Subj: CERTIFICATION OF TRAINING AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

Ref: (a) COMNAVRESFORINST 5510.9(Series)
     (b) SECNAV M-5510.36, Department of the Navy Information Security Program
     (c) SECNAV M-5510.30, Department of the Navy Personnel Security Program

1. I have completed the (specify the course of instruction) as required by reference (a). I am fully aware of the duties and responsibilities of the position per references (b) and (c) chapter 2. A complete inventory of the command’s classified holdings has been accomplished and (specify if all material has been accounted for and if any discrepancies exist in the program).

2. I have assumed responsibilities for all classified materials and will ensure accurate and complete accountability of all classified materials held by the command.

(SIGNATURE)

Enclosure (1)
From: Command/Organization Name
To: (Rank, Name of Appointee)

Subj: APPOINTMENT AS COMMAND TOP SECRET CONTROL OFFICER/ASSISTANT TOP SECRET CONTROL OFFICER

Ref: (a) SECNAV M-5510.36, Department of the Navy Information Security Program
(b) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(c) COMNAVRESFORINST 5510.9

1. In accordance with the references, you are hereby appointed as the Command/Organization Name Top Secret Control Officer.

2. You are directed to familiarize yourself with references (a) through (c) and other applicable directives pertaining to this appointment.

3. You are directed to conduct a joint inventory of the classified material or other accountable material in custody and report in writing the results to the Security Manager (SM) no later than ____________.

Signature

Copy to:
Chief of Staff
Command SM

Enclosure (1)

C-1
COMNAVRESFORINST 5510.9A
6 Feb 14

APPENDIX E

Generic Security Briefing

SECURITY BRIEFING

1. Your assignment to the Command comes with the responsibility
to safeguard all classified material you come in contact with.
To fulfill your responsibilities and maintain security you are
required to observe the following rules.

   a. Do not discuss classified information with unauthorized
   persons or individuals that do not need the information in the
   performance of their duties. If in doubt about someone’s need
   to know ask your supervisor or the Security Manager.

   b. Never discuss classified information over a non-secure
   telephone. Secure telephones are available to discuss
   classified information. See your supervisor for the location of
   the nearest secure telephone.

   c. Never leave classified information unprotected. It must
   either be properly stored or in the custody of a cleared person.
   Classified information will be marked to show the level of
   classification (i.e., top and bottom portion etc.)

   d. Do not read or discuss classified information in a non-
   secure area.

   e. Do not remove classified information from the command
   without specific permission. If you need to hand carry
   classified material, contact your supervisor and the security
   office to obtain a courier card or a courier letter.

   f. Classified information may only be reproduced on copier
   machines specifically authorized for use with that particular
   level of classified material. All copy machines are marked to
   indicate the highest level authorized for that machine.

   g. Do not send classified information out of the command by
   other than approved methods. The U.S. Postal Service registered
   mail service is used to send secret and below material within
   the U.S. and its territories.

Enclosure (1)

E-1
You must first see the security office before sending classified material outside the contiguous United States and for classified material above secret.

h. Classified material may only be destroyed using an approved shredder. All paper documents/products at the command regardless of classification will be shredded to include handwritten notes. The only items to be placed in command trash cans are food items, candy wrappers and items of this nature. Approved shredders are easily accessible and located in all work spaces. Contact the Command Security Office for additional guidance.

i. Do not store security container combinations in non-secure places (i.e. wallets, under desk, calendars, etc).

j. You will be issued a proximity badge for building access. It is required that you show your badge to the quarterdeck watch when entering the building. Handle your badge carefully, as you would any other high value card, such as a credit card. Report lost, damaged or stolen cards to the Security Manager immediately.

k. Security folders, envelopes or magnetic media containing classified material must be clearly marked.

l. During normal working hours, classified material on desks and in the “in” baskets should be placed faced down or in a folder when not in use; classified cover sheets should be used especially for documents and messages being routed and transferred within the Command.

m. Upon securing for the day, all desks are to be clear of classified information. Tumbler locks on safes are to be spun at least four times and drawer handles pulled to ensure that containers are locked. Ensure your doors are locked at the end of the day and complete and initial the SF-701.

n. The Security Container Form, SF-702, must be signed when opening and closing the safe.

2. Any person discovering unprotected classified information or an unauthorized disclosure of classified information has two immediate responsibilities.
a. Attempt to protect the classified information from further compromise.

b. Report the circumstances to a responsible security official. If you cannot do both, have someone else make the report while you continue to protect the information.

3. Most security violations have occurred due to carelessness, insufficient knowledge of security regulations, indifference, lack of security consciousness or ignorance of the penalties involved. A successful security program at this command is dependent upon how well each individual carries out his or her responsibilities. Effective security can be maintained only with your full cooperation.

4. Personnel with access to classified information and a valid clearance will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position.

5. Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported.

I have read this briefing and understand my security responsibilities.

Print: (Name, First, MI, Last)

Signature/Date

Security Representative

Enclosure (1)
APPENDIX F

"Command Name"

Indoctrination/Orientation Brief

1. Nature of Classified Information. Classified information is information that requires protection against unauthorized disclosure in the interest of national security and is classified under one of three designations: Top Secret, Secret or Confidential depending on the level of sensitivity. Designations authorized to identify classified information are listed below:

   a. "TOP SECRET" is applied to information or material of which unauthorized disclosure could reasonably be expected to cause "exceptionally grave damage" to national security. Examples include, national defense plans, cryptologic and communications intelligence systems, sensitive intelligence operations or disclosure of scientific or technological developments vital to national security.

   b. "SECRET" is applied to information or material of which the unauthorized disclosure could reasonably be expected to cause "serious damage" to national security. Examples include programs or policies directly related to national security, significant military plans or intelligence operations or compromise of scientific or technological developments relating to national security.

   c. "CONFIDENTIAL" is applied to information or material of which the unauthorized disclosure could reasonably be expected to cause "damage" to national security. Examples include the compromise of information that indicates strength of ground, air and naval forces or technical information used for training, maintenance and inspection of classified munitions of war.

2. Protection of Classified Information. As a custodian of classified information, you have a personal, moral and legal responsibility at all times to protect and control classified information oral or written. Further, you must follow procedures to ensure unauthorized persons do not gain access to classified information.

   a. Classified material must be stored in approved vaults, safes or open storage areas and classified waste material must be shredded.

Enclosure (1)
b. All paper documents/products at the Command will be shredded to include handwritten notes. The only items to be placed in command trash cans are food items, candy wrappers and items of this nature. Approved shredders are easily accessible and located in all work spaces. Contact the Command Security Office for specific instructions.

c. Cover sheets will be used on all classified materials to protect the contents from disclosure.

3. Security of Personal Work Area. Individuals are responsible at all times for ensuring against unauthorized disclosure of classified information within his/her personal work area. During all periods when workspaces are not occupied, classified material will be locked in approved storage containers; a locked room does not constitute adequate security storage.

4. Reproduction of Classified Material. Reproduction of classified material is subject to the same control as the original document. Classified material, Secret/Confidential will not be reproduced without approval on copier machines. Top Secret material will not be reproduced without the approval of the originator or higher authority.

5. Telephone Procedures. Classified material will not be discussed on the telephone unless a secure telephone unit third generation is used in the secure mode. Ask the Communication Security Custodian for assistance.

6. Authorized Disclosure. You must check the identity, the clearance, the need to know (official need for access) and the ability to properly protect (or store) the information before passing classified information to anyone. No one has a right to have access to classified information solely by virtue of rank or position. Need to Know determines whether an individual's official duties require possession or access to classified information. The authority to release classified material rests with the individual who has control of the information and not on the prospective recipient. Classified information may be disclosed only to authorized individuals.

7. Unauthorized Disclosure. Unauthorized disclosure of classified information may result in disciplinary action. Such action may include a warning notice, formal reprimand, suspension without pay, forfeiture of pay, court martial, discharge, fine and/or imprisonment.

Enclosure (1)
8. Unauthorized Contact. Report any attempt by unauthorized personnel to obtain classified information to the security office.

9. Mailing Classified Materials. Secret and Confidential materials may be mailed via U.S. Postal Service registered mail within and between the U.S. and its territories. You must contact the security office for specific instruction on shipping secret and/or confidential outside the continental U.S. and packaging of top secret. Top secret material can only be transported by Defense Courier Service.

10. Hand Carry of Classified Materials. Classified materials will not be hand carried to or from the Command unless the individual has a DD Form 2501, Courier Authorization Card or courier letter. This includes transporting items by government vehicle, privately owned vehicle or by air. Please contact the security office for instructions.

11. Foreign Travel. Travel to overseas location requires a Defense Security Briefing. Please contact the security office prior to any travel outside of the U.S.

12. Compromise of Classified Materials. All suspected compromises of classified materials will be reported to the security office as soon as they are detected. This includes adverse personal information that could reflect on the trustworthiness of individuals with access to classified information.

13. Prohibited Items. Articles or items such as firearms, ammunition or explosives which may present potential security or safety hazards should be limited to approved areas as prescribed by the CO. In an open storage area (also called a secure room) or certified spaces which process classified information, security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth to prevent access by unauthorized persons. Use of cell phones, PDEs, mp3 players, 2-way pagers, any device that retains, stores or transmits information or which include wireless capability is prohibited in spaces which process classified material. Introduction of these devices into U.S. Government systems allows for the creation of a vector across classification boundaries.
Subversion and Espionage Directed Against The United States

1. Usually, U.S. citizens give certain indicators when they attempt to commit or are committing espionage. The indicators are as follows:
   a. Abuse of the need to know principle
   b. Changes in lifestyles.
   c. Removal of classified material.
   d. Undue affluence.
   e. Excessive use of copy machines.
   f. Personality changes.
   g. Habitual overtime or unusual hours.

2. Individuals whose behavior is suspicious should be reported immediately to the SM.

3. Under regulations, the following incidents must be reported immediately:
   a. Attempts by unauthorized persons to obtain classified or unclassified information concerning defense facilities, activities, personnel or material.
   b. Attempts by unauthorized persons to obtain information through photographs, observation, collection and documents or other means.
   c. Incidents where defense personnel or family members are subject to questions about duties or are threatened, coerced or pressured to cooperate with a foreign intelligence service or agent.
   d. Any information regarding incidents of known, suspected or possible espionage or international terrorism.
   e. Any knowledge you obtain regarding acts of deliberate compromise of classified information, either committed, attempted or contemplated.
f. Non-official contacts by defense personnel with:
   (1) Known or suspected members of a foreign intelligence service.
   (2) Foreign military police organizations.

g. Official contacts by foreign intelligence and police when they:
   (1) Show undue curiosity about a DoD service or employee.
   (2) Attempt to obtain classified information.
   (3) Attempt to establish any type of friendship, social or business relationship outside the range of normal official duties.

REPORT ANY OF THE ABOVE SUSPICIONS OR INCIDENTS IMMEDIATELY TO THE SECURITY OFFICE. IF THERE ARE ANY QUESTIONS CONCERNING THIS MATERIAL PLEASE CONTACT THE SSO/COMMAND SECURITY OFFICE.

I acknowledge reading the above information and will notify the Security Office of any changes to my personal security status or foreign contacts.

_________________________________  ___________________________________  ____________
PRINT  SIGN  DATE

Enclosure (1)
APPENDIX H

Security Access Eligibility Report

Date: 
UIC

ASSIGNED TO:

From: Department Head/Supervisor
To: Director, Central Adjudication Facility
Via: Commanding Officer organization Name

Subject’s Name and Rank/Grade:

Current Indoctrination Status: (YES/NO)

Current Debrief Status: ___ CAUS: ___ SUS: ___ DATE: ___

Current Duty Station/Assignment:

Reason for Report:

PART I: Check appropriate response for each question and provide explanatory details under comments for any Yes answer(s).

1. Has the subject been arrested, detained or been a party to a civil or criminal action by either military or civilian authorities within the past 2 years? ___ NO ___ YES

2. Has the subject been awarded any nonjudicial punishment not previously reported? ___ NO ___ YES

3. Has the subject been reported for an infraction or violation of any security regulation? ___ NO ___ YES

4. Has the subject had any known significant contact with foreign nationals? ___ NO ___ YES

Enclosure (1)
5. Has the subject been involved in any way with the use of marijuana, drugs, abuse of prescription or non-prescribed drugs?  
   __ NO   __ YES

6. Has the subject been treated for any illness related to a nervous, emotional or mental disorder?  __ NO   __ YES

7. Has the subject demonstrated any evidence of frequent, habitual or compulsive gambling?  __ NO   __ YES

8. Is the subject known to have any excessive indebtedness or recurring financial difficulties?  __ NO   __ YES

9. Does the subject display any signs of an unusually high standard of living or any unexplained affluence as illustrated in APPENDIX G of reference (b)?  __ NO   __ YES

10. Has the subject been repetitively absent from duty or habitually late for duty?  __ NO   __ YES

11. Has the subject shown any indications of sexual practices that might be interpreted or construed as being in any way abnormal?  __ NO   __ YES

12. Has the subject been involved in the possible or probable compromise or unauthorized disclosure of SCI or other classified material?  __ NO   __ YES

13. Has the subject’s access to SCI been denied, revoked or suspended during the reporting period?  __ NO   __ YES

14. Has the subject shown signs of habitually using alcohol to excess?  __ NO   __ YES

15. Do you know of anything which might reflect adversely upon subject’s loyalty to the United States?  __ NO   __ YES

COMMENTS: (Identify question and provide details. Use a separate piece of paper if necessary.)

PART II: Include observations on the subject’s character and stability which should be considered in a determination of SCI access eligibility.

Enclosure (1)
1. Excellence of character (subject’s trustworthiness, reliability, dependability, discretion and moral values):

2. Stability (subject’s maturity, temperament, general attitude toward authority and ability to work with others):

3. Other comments/observations:

4. Include documentation or evidence, if available.

PART III. Command recommendation regarding eligibility for continued access to classified information. (If eligible, under what conditions, e.g., observation, probation or further action.)

Signature Block
Title

Copy to:
Files

Enclosure (1)
Personnel Security Reporting Requirements

Because of your job, you have been granted special access to sensitive and classified information that is vital to the nation's security. You are charged with safeguarding that information. It is both an honor and a privilege that allows you to make a very special contribution to your country. But it's a privilege that carries with it certain obligations; you must meet these obligations in order to maintain your access.

One of your obligations is to report to your Security Manager those behaviors, incidents or events that might in some way impact national security and your ability or that of your co-worker, to function positively and effectively in a national security environment.

You Must Report:

Foreign Travel

- Business or personal (vacation, family emergency, etc.)
- Report your trip in advance as necessary and follow up with security upon your return. (Reporting all foreign trips in advance in which a pre-travel defensive security briefing is requested/required or if travel is to a HOT SPOT country).

Foreign Contact

- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard suspicious.
- Contact with anyone who works for or is associated with foreign government (including a foreign embassy) or foreign-owned organization or business
- Close or continuing contact with a foreign national, in any capacity: in person, by telephone, over the Internet, etc. (A foreign national with whom one has continuing contact may be a relative, stranger, a business or work associate or someone quite close to you such as a boyfriend/girlfriend, relative's spouse or a friend of the family)
Financial obligations, investment in or employment with foreign nationals and companies.

**Counseling**

- Any consulting with a mental health professional (psychiatrist, psychologist, counselor, etc) NOT to include the following (unless they are court-ordered):
  - Strictly marital, family or grief counseling not related to violence by you.
  - Strictly related to adjustments from service in a military combat environment.
- Prescribed drugs for treating mental health conditions.

**Drug Use**

- Illegal/improper use of narcotics, non-medicinal drugs, non-prescription drugs or controlled substances.
- Previously unreported drug use.
- Misuse of or addictions to prescription drugs.

**Criminal Conduct**

- All arrests (regardless of whether or not there is a conviction).
- Knowledge of a criminal act by another accessed individual.
- Knowledge of a criminal act by a member of your immediate family or a close relative.
- Attempted coercion or blackmail.

**Alcohol Incidents at Work or Home**

- Arrests.
- Treatment.
- Counseling.

**Financial Concerns**

- Excessive indebtedness.
- Liens.
- Collections.
- Bankruptcies.
- Garnishments.
- Judgments.
- Unexplained financial affluence.
Improper Security Practices

- Inadvertent or deliberate removal of classified information/materials to an unauthorized area.
- Inadvertent or deliberate unauthorized destruction of classified information/materials.
- Knowledge of a security violation or infraction (not reporting it).
- Inoperability of locks, doors, vaults, etc., that are in place to secure classified information/materials.
- Deliberate or inadvertent disclosure of classified information/materials to an unauthorized person.
- Loss of classified information/materials.
- Request for classified or sensitive information/materials through unauthorized channels.

Computer/Automated Information Systems Misuse

- Unauthorized entry into an AIS system, whether government or contractor, for any reason.
- Modification, destruction or manipulation of hardware or software, whether government or contractor equipment.
- Password Misuse.
  - Obtaining/using someone else’s password to browse through another’s account without permission.
  - Sharing a password.
  - Copying/deleting information from another’s account without their permission.

Suspicious Incidents

You may make your report to your security officer via e-mail, facsimile, telephone or in person. Telephonic or in-person reporting must be followed by a written report. All information about the incident should be reported as soon as possible.

Clearly, we are unable to list all possible eventualities for each general heading. If you are in doubt as to whether or not a behavior, incident or event should be called to the attention of the Security Manager, just report it. Your Security Manager is in the best position to make a determination of the risks and to help mitigate or resolve them.
Make the Right Choice Just Report It!

REPORTABLE ITEMS AND CIRCUMSTANCES

- Potential Espionage Indicators Appendixed by Others
  - Unexplained affluence.
  - Keeping unusual work hours.
  - Divided loyalty or allegiance to the U.S.
  - Disregarding security procedures.
  - Unreported foreign contact and travel.
  - Pattern of lying.
  - Attempts to enlist others in illegal or questionable activity.
  - Verbal or physical threats.
  - Inquiry about operations/projects where no legitimate need to know exists.
  - Unauthorized removal of classified information.
  - Fraud/Waste/Abuse of government credit cards and/or travel or training advances.
  - Habitual visitor(s) collecting data at various offices, about command's strengths, alarms, recall rosters and/or high ranking staff members.

Security is a team effort. Your diligence in promptly reporting concerns and adhering to your agency's security policies and procedures will ensure the integrity of national security. As a team, we can protect our war fighters, colleagues and families from potential harm.

PRINT NAME: ____________________________________________

DATE: __________

SIGNATURE: ____________________________________________

SECURITY OFFICIAL SIGNATURE: ____________________________

Enclosure (1)
APPENDIX J

"Command Name"

Employee’s Outside Employment/Activities

Potential conflict with an individual’s responsibility to protect classified material may arise from outside employment or other outside activity from contact or association with foreign nationals. In cases where such employment or association has resulted in a suspected or established compromise of classified material, the local security official and supporting activity must be advised immediately. Involvement in non-U.S. government employment or activities that raise potential conflicts with an individual’s responsibility to protect classified information is of security concern and must be evaluated by a security official to determine whether the conflict is of such a nature that classified access should be denied or revoked. Individuals who hold or are being considered for classified access approval must report in writing to the local security official any existing or contemplated outside employment or activity that appears to meet the criteria listed below. In addition, initial or updated personal history statements must include details of outside employment or activities.

1. Employment that must be reported includes compensated or volunteer service with any foreign national; with a representative of any foreign interest; or with any foreign, domestic or international organization or person engaged in analysis, discussion or publication of material on intelligence, defense or foreign affairs.

2. Continuing association with foreign nationals must be reported.

3. When an individual’s outside employment or activity raises doubt as to an individual’s willingness or ability to safeguard classified information, he or she will be advised that continuing that employment or activity may result in withdrawal of SCI access and be given an opportunity to discontinue.

4. Individuals will immediately report in writing to their local security officer any existing or contemplated outside employment or activity that appears to meet the above criteria.

Enclosure (1)
Written reports must be submitted before accepting outside employment or activity.
APPENDIX K

"Command Name"

Personal Attestation Policy

I accept the responsibilities associated with being granted access to classified National Security Information. I am aware of my obligation to protect classified National Security Information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official need to know. I further understand that, in being granted access to classified information and Sensitive Compartmented Information, a special confidence and trust has been placed in me by the U.S. Government.

EMPLOYEE SIGNATURE __________________________ PRINT NAME __________ DATE __________

WITNESS SIGNATURE __________________________ PRINT NAME __________ DATE __________

WITNESS SIGNATURE __________________________ PRINT NAME __________ DATE __________
From: Organization
To: Individual’s First and Last Name, USN
Subj: SUSPENSION OF ACCESS FOR CAUSE
Ref: (a) SECNAV M-5510.30
Encl: (1) Acknowledgement of Receipt
      (2) Administrative Remarks (NAVPERS 1070/613)
      (3) Security Debriefing Acknowledgement, Security
          Termination Statement (OPNAV 5511/14)

1. Effective the date of this letter, you are being debriefed for cause from all classified information for reason for suspension of access to classified information. This action is consistent with the interests of national security.

2. The decision regarding retention of clearance eligibility will be referred to the Department of the Navy, Central Adjudication Facility (DONCAF). You are reminded that the non-disclosure agreement, you signed prior to your access to classified information remains in effect.

3. You will be notified in writing if your access to classified information is reinstated.

4. Please contact ____________, Security Manager, at ________ regarding any questions or comments.

Copy to:
DONCAF
Security

Enclosure (1)

L-1
From: Individual’s First and Last Name, USN
To: Commander, Navy Reserve Forces Command

Subj: ACKNOWLEDGEMENT OF RECEIPT

1. I acknowledge receipt of the letter notifying me that my access has been suspended.

________________________  _____________________  _____________________
PRINT                    SIGN                          DATE

Enclosure (1)
APPENDIX M

NATO Security Briefing

FOREWORD

This sample security briefing contains the minimum elements of information that must be provided to individuals upon initial indoctrination for access to NATO classified information. This briefing is intentionally general so it may be used by all U.S. Government agencies and contractors. Agencies and contractors are encouraged to expand upon this briefing to accommodate specific situations. There is no requirement to copy this format or literary style; however, the minimum elements contained herein shall be included. Detailed procedures are contained in United States National Security Authority for NATO (USSAN) Instruction 1-69, NATO's CM(2002) 49 "Security within NATO" and its Supporting Security Directives (AC/35-D/2000 through D/2005), USSAN Instruction 1-70 (Industrial Security) and the National Industrial Security Program Operating Manual (NISPOM).
APPENDIX N

NATO/ATOMAL Security Briefing

INTRODUCTION

You will require access to NATO classified information in pursuance of your current duties. The security standards and procedures for handling and protecting NATO information are in some cases different than those for U.S. information. This briefing explains the basic security standards and procedures for safeguarding NATO information.

WHAT IS NATO?

NATO is an acronym for the North Atlantic Treaty Organization. Member nations have signed the North Atlantic Treaty and the NATO Security Agreement, which obligate them to comply with NATO rules. The following nations are members of NATO:

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Hungary</td>
<td>Portugal</td>
<td>Turkey</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>Canada</td>
<td>Italy</td>
<td>Spain</td>
<td>Norway</td>
<td>Estonia</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Luxembourg</td>
<td>United Kingdom</td>
<td>Iceland</td>
<td>Latvia</td>
</tr>
<tr>
<td>Germany</td>
<td>Netherlands</td>
<td>United States</td>
<td>France</td>
<td>Lithuania</td>
</tr>
<tr>
<td>Greece</td>
<td>Poland</td>
<td>Denmark</td>
<td>Romania</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Albania</td>
<td>Croatia</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Secretary of Defense is the United States National Security Authority for NATO. As such, he is responsible for ensuring that NATO security requirements are implemented throughout the Executive Branch of the United States Government.

WHAT IS NATO INFORMATION?

NATO information is information that has been generated by or for NATO or member nation national information that has been released into the NATO security system. The protection of this information is controlled under the NATO security regulations and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

Material received by an agency direct from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation.

Enclosure (1)
If it has been marked "NATO" by the originating nation, it must be assumed to contain information released to NATO and it is controlled under the NATO Security Program. If the material has a national classification marking and is not marked "NATO" by the originator, DO NOT apply a NATO marking unless you are informed in writing by the originator that the material is intended for NATO and is to be protected under the NATO Security Program. Moreover, the material or the information therein shall not be released into the NATO system without the prior written consent of the originator.

"RELEASABLE TO NATO" statements on U.S. material indicate that the information contained therein has been authorized under applicable disclosure policies for release to NATO and may be discussed within the NATO community. Only the copies that are being released to NATO shall be marked with a NATO marking. They are to be dispatched and controlled in the NATO registry system or per guidance provided by the supporting sub-registry or control point. The remaining copies shall continue to be controlled as U.S. information. There must be a record, however, that the information has been authorized for release to NATO.

CLASSIFICATION MARKINGS AND CATEGORIES OF NATO INFORMATION

NATO has four levels of classified information: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL and NATO RESTRICTED. Certain NATO information is further categorized as ATOMAL information. NATO also distinguishes official, unclassified information. The markings and categories of NATO information are described below.

COSMIC TOP SECRET (CTS) - This security classification is applied to information the unauthorized disclosure of which would cause exceptionally grave damage to NATO. (NOTE: The marking "COSMIC" is applied to TOP SECRET material to signify that it is the property of NATO. The term "NATO TOP SECRET" is not used).

NATO SECRET (NS) - This security classification is applied to information the unauthorized disclosure of which would cause serious damage to NATO.
NATO CONFIDENTIAL (NC) - This security classification is applied to information the unauthorized disclosure of which would be damaging to the interests of NATO.

NATO RESTRICTED (NR) - This security classification is applied to information the unauthorized disclosure of which would be disadvantageous to the interests of NATO. (NOTE: Although the security safeguards for NATO RESTRICTED material are similar to those of FOR OFFICIAL USE ONLY, OFFICIAL USE ONLY or SENSITIVE, BUT UNCLASSIFIED information, "NATO RESTRICTED" is a security classification).

ATOMAL - ATOMAL information can be either U.S. Restricted Data or Formerly Restricted Data that is classified pursuant to the Atomic Energy Act of 1954, as amended or United Kingdom ATOMIC information that has been officially released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA) or NATO CONFIDENTIAL ATOMAL (NCA).

NATO UNCLASSIFIED (NU) - This marking is applied to official information that is the property of NATO, but does not meet the criteria for classification. Access to the information by non-NATO entities is permitted when such access would not be detrimental to NATO. In this regard, it is similar to U.S. Government official information that must be reviewed prior to public release. (As of mid-2002, NATO has required its classified information to be portion-marked, i.e. with a classification marking applied to each paragraph heading, etc.).

ACCESS AUTHORIZATION

NATO Classified Information - Your security official will inform you of your level of access to NATO classified material and whether you are authorized access to ATOMAL information (see below). Additionally, your agency should maintain a list indicating the levels of access for each assigned individual who is authorized access to NATO information for you to verify NATO access authorizations for other employees.

As with U.S. information, access is NOT based on duty position, rank or level of clearance. Access is based on need to know, the proper level of U.S. clearance and an access briefing for a specific level and type of NATO/ATOMAL information. Remember, it is your responsibility to ensure that an individual is authorized access to a particular type and level of classified NATO and/or ATOMAL information before you provide access.
This responsibility applies to all modes of transmission, e.g. oral, written, visual and electronic. If in doubt, seek assistance from your security officer or NATO sub-registry or control point. NATO information is provided to non-NATO nationals and entities only with the approval of the originator of the information. That approval is gained through the appropriate NATO committee.

**ATOMAL Information** - An employee of the DOD or its contractors may be granted access to ATOMAL information only if the employee has a need-to-know to perform his or her job and has been appropriately cleared and briefed for access to Restricted Data. An employee of NASA may be granted access to ATOMAL information concerning aeronautical and space activities, if the individual is cleared for access to Restricted Data. All other individuals and NASA employees requiring access to ATOMAL information other than that covering aeronautical and space matters, shall have a "Q" clearance issued by the Department of Energy. Interim clearances shall not be accepted as the basis for access to ATOMAL information.

**THE REGISTRY SYSTEM**
A Central Registry has been established by each NATO member nation to ensure proper control and accountability of NATO classified documents. Central United States Registry (CUSR) is located in Room RDF1J664A, the Pentagon, Washington D.C. As an official representative of the U.S. Security Authority for NATO, the CUSR oversees the administration of the U.S. registry system. The CUSR establishes all U.S. sub-registries to execute the accountability and security management of NATO and ATOMAL material at various U.S. locations throughout the world. Based on location and volume of material, control points may be established to assist in these operations.

**ACCOUNTING FOR NATO CLASSIFIED MATERIAL**

**COSMIC TOP SECRET, NATO SECRET and all ATOMAL** - Receipts and logs shall be maintained on the receipt, disposition, destruction and dispatch of COSMIC TOP SECRET, NATO SECRET and all ATOMAL material. In addition, each individual is required to execute a disclosure record upon acquiring access to each item of CTS/CTSA material or ATOMAL with special limitation restrictions.
**NATO CONFIDENTIAL and NATO RESTRICTED.** You are required to maintain administrative control of NATO CONFIDENTIAL and NATO RESTRICTED material adequate to preclude unauthorized access. Specific accounting records are not necessary unless they are required by the originator.

**MARKING AND ACCOUNTING FOR U.S. DOCUMENTS CONTAINING NATO CLASSIFIED INFORMATION**

A newly generated U.S. classified document that contains NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or U.S. classified information it contains. Declassification and downgrading instructions shall indicate that the NATO information is exempt from downgrading or declassification without the prior consent of NATO; the reason to be cited is "foreign government information." The statement "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION" will be affixed to the front cover or first page, if there is no cover. Portions that contain NATO classified information shall be marked to identify the information (e.g., NS). The document shall be accounted for, safeguarded and controlled as specified for NATO documents of the same classification. If a record is required for the NATO classification information, a U.S. document containing the NATO information will be logged, accounted for and handled in the same manner as required for the NATO information. However, NATO reference numbers are not required. A record shall be maintained of source NATO documents, as required for derivatively classified U.S. documents. Existing U.S. documents that do not meet this requirement shall be marked and handled according to these procedures when they are removed from the files for use. AIS storage media shall be handled as described in C-M (2002)49 and its supporting directives and in Section X of USSAN 1-69.

**SAFEGUARDING NATO MATERIAL**

**General.** The physical security requirements for material marked NATO CONFIDENTIAL and above are the same as for U.S. material of the same level of classification. NATO RESTRICTED material may be stored in a locked filing cabinet, book case, desk or other such container or in a room or building that is locked during non-duty hours, provided access to the room or building is controlled so that only authorized personnel can gain access to the information.
All personnel with access to a security container that is used to store NATO information must be briefed and authorized access to the level and type of NATO information that is stored in that container.

**Segregation.** You are required to ensure that NATO and non-NATO material are filed separately. ATOMAL material must be filed separately from non-ATOMAL material. This may be accomplished by using a separate security container or to conserve storage space, by using separate drawers or file dividers in the same security container holding U.S. classified material. Additionally, you are required to segregate ATOMAL control records from non-ATOMAL control records.

**Combinations.** Combinations to security containers containing NATO classified material must be changed at least annually, upon departure of an individual with access to the combination or if the combination has been or is suspected of having been compromised.

**Transmission.** The national or international transmission of CTS and CTSA material shall be through the registry system using a cleared government courier service; for example, diplomatic pouch or military courier service. The national and international transmission of NS, NSA, NC and NCA shall be by cleared courier or by appropriately cleared and briefed employees who possess courier identification and authorization or by U.S. registered mail using the same provisions as prescribed for U.S. classified material.

Receipts are required for CTS, NS and all ATOMAL material. NC may also be sent by U.S. First Class mail between U.S. Government activities within the United States. In urgent situations, the United States Postal Service Express Mail may be used to transmit material NS and below within the U.S., its Territories and the District of Columbia. However, there are restrictions on the use of Express Mail; guidance should be sought from your security officer or sub-registry or control point. NR material may be sent by U.S. First Class mail within the U.S. and to an APO/FPO or NATO address through the U.S. or NATO member nation postal service.

**ATS.** Systems must be accredited specifically to handle NATO classified information.

Enclosure (1)
Organizations with AIS systems accredited for handling NATO classified information must issue instructions for processing, handling and accounting for NATO classified information. Be sure you receive a copy of those instructions and apply them.

**Destruction.** The destruction of CTS, CTSA, NS, NSA and NCA material will be accomplished only by registry system personnel using a destruction certificate and a method approved for the destruction of U.S. material of the same level of classification. NATO RESTRICTED and NATO CONFIDENTIAL shall be destroyed by any means authorized for U.S. CONFIDENTIAL material.

**Reproduction.** COSMIC documents shall be reproduced by the CUSR and COSMIC Sub-registries which must report the number of copies made to the CUSR. Reproduction of ATOMAL (CTSA, NSA and NCA) shall be made only by the CUSR, ATOMAL Sub-registries and ATOMAL Control Points. Reproduction of NATO Secret and below may be produced by the addressee under strict need-to-know principle and provided that the originator has not restricted reproduction. Reproduced copies shall be accounted for and safeguarded in the same manner as the original.

**SECURITY VIOLATIONS AND POSSIBLE LOSS/COMPROMISE OF NATO CLASSIFIED MATERIAL**

**General.** NATO guidelines are very similar to those used for U.S. material. However, the servicing sub-registry or control point must be informed of the incident, in addition to the responsible security or counterintelligence officials.

**Procedures.** If you find NATO material unsecured and unattended, immediately contact your security officer or registry system official. Stay with the material and wait for the security officer or registry official to arrive. Do not disturb the area or material. Do not allow anyone else to disturb the area or allow unauthorized personnel to have access to the material. If it is necessary that you leave the area before your security officer or registry system official can assume custody, place the material in a security container and lock the container. If the container is already locked and you are not authorized access or there is no container, take the material directly to an appropriately cleared security or registry system official, explain the circumstances and obtain a receipt for the material.
Espionage, sabotage, terrorism and deliberate compromise. Information concerning a deliberate compromise of NATO/ATOMAL material, attempted or actual espionage directed against NATO/ATOMAL information or actual or planned terrorist or sabotage activity against facilities or users of NATO classified material, shall be reported promptly to your security officer or to your agency's counterintelligence officer or the Federal Bureau of Investigation. The following are typical reportable situations:

a. Attempts by unauthorized persons to obtain classified information concerning NATO or U.S. facilities, activities, personnel or material through questioning, elicitation, bribery, threats or coercion, either by direct or indirect contacts or correspondence.

b. Attempts by unauthorized persons to obtain classified information through photographing, wiretapping, eavesdropping, observation or by any other means.

c. Attempts by persons with known, suspected or possible foreign intelligence backgrounds, associations or activities to establish a friendship or a social or business relationship or to place you under obligation through special treatment, favors, gifts, money or other means.

d. Information concerning terrorist plans and activities posing a direct threat to U.S. or NATO facilities, activities, personnel or material.

e. Known or suspected acts or plots to harm or destroy U.S. or NATO property by sabotage. Anyone with access to NATO classified information could be a potential target. If you become aware of activities such as those as described above or someone approaches you directly to engage in such activities, remember the following:

(1) Stay calm. You are not at fault because they chose to target you.

(2) Be noncommittal. Be ambiguous as to whether or not you will provide them with material or information.
(3) Report it promptly. Even if it seems purely coincidental or insignificant, a small detail may be the key to identifying and countering espionage or sabotage or a terrorist act. Do not discuss the incident with friends, family, co-workers, etc., unless directed to by your security officer or counterintelligence representative.

(4) It is never too late! If you have provided material or information to an unauthorized recipient, Report it.

FOREIGN TRAVEL

Your personal travel will not be limited based solely on the fact that you have access to NATO classified information. There are, however, risks involved in travel to certain countries. Check with your security officer for advice and assistance. If you choose to travel to high-risk countries, you are required to coordinate with your leave/travel order granting authority and security office and obtain a travel security briefing. Upon your return, you should report any incident that may have been an attempt to collect sensitive information.

WHERE DO I GO FOR MORE HELP?

If problems or specific questions arise concerning NATO classified information, your security officer and sub-registry/control point can assist you. Further information is also available to users in (.mil) and (.gov) domains on the Central U.S. Registry website.

NIPRNET website is https://secureweb.hqda.pentagon.mil/cusr.
SIPRNET website is http://classweb.hqda-s.army.smil.mil/cusr.
Protection of Hand-Carried, Classified Material in a Travel Status Courier Briefing

1. You are designated as a Command Courier and authorized to hand-carry or transport documents or equipment classified (Secret) maximum distance (200) miles to and from your command to approved designated location in the performance of your official duties. This authorization does not include hand carrying classified material or equipment aboard commercial aircraft. You will familiarize yourself with the following provisions:

   a. Classified material must be in your physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (Continental U.S. only) is available. Hand-carrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage at a government activity or a cleared contractor facility. When you surrender any package containing classified material for temporary storage (e.g., overnight or during meals) you must obtain a receipt signed by an authorized representative of the contractor facility or Government installation accepting responsibility for safeguarding the package.

   b. Classified material shall not be read, studied, displayed or used in any manner in public conveyances or places.

   c. When the classified material is carried in a private, public or government conveyance, it shall not be stored in any detachable stowage compartment such as a trailer, luggage racks, aircraft travel pod or drop tank. You may not take classified material to your home.

2. A list of all classified material carried or escorted by you will be maintained by your command. Upon your return, you must account for all classified material.

3. Whenever possible, you should return the classified material to your command by one of the other approved methods of transmission.
Upon return, the courier shall return all classified material in a sealed package or, for any classified material that is not returned, produce a receipt signed by the security officer of the addressed organization.

4. Things to be aware of:
   a. You must ensure that the material is not available at the temporary duty location.
   b. You must ensure that all necessary transfer documentation is completed.
   c. No overnights with classified material are authorized.
   d. A specific Letter of Authorization is required, in addition to the Courier Authorization Card, when travel involves the use of commercial aircraft.
   e. The Command SM’s office will be notified if classified material is to be carried onboard a commercial aircraft.
   f. Upon transfer from your command, the DD 2501 will be turned-in to the Command SM’s office.
   g. This briefing will be conducted upon initial issue of a Briefing Card returned on file. The Briefing Card will be reissued every 2 years.

5. If a search of your person and belongings is required by proper authority, take these steps:
   a. Permit search by any method that does not compromise or destroy classified material in your possession or
   b. If material being carried would be destroyed or compromised by the usual search methods, request appropriate inspecting official to verify your official status with this command by contacting (xxx) xxx-xxxx.
I acknowledge receipt of briefing and DD 2501.

__________________________  ______________________  _______________
PRINT                  SIGN                   DATE

__________________________
PRINT/TYPe NAME DIRECTORATE

FOR YOUR COMMAND TO FILL IN CARD NO#: __________________

ISSUE DATE: ____________________
APPENDIX P

SAMPLE

Authorization to Hand-Carry Classified Material Onboard

(Letterhead Paper)

From: Commander,
To: (Rank, Name and SSN of individual hand-carrying material)

Subj: AUTHORIZATION TO HAND-CARRY CLASSIFIED MATERIAL ABOARD COMMERCIAL AIRCRAFT

Ref: (a) SECNAVINST 5510.36(Series)

1. It has been determined that an operational commitment exists that necessitates the hand-carrying of classified material aboard a commercial aircraft; you are hereby authorized to hand-carry subject classified material.

2. You are directed to familiarize yourself with reference (a) prior to departure.

3. The following items provided are required per reference (b):

   a. Rank, Full Name, Branch of Service, SSN and command address.

   b. When required, you will present description of individual's ID, e.g., "U.S. Armed Forces Identification Card, DoD PN ID No. 222-22-2222."

   c. The material being carried is described as (Give description, e.g., 1, 8½ x 11” envelope)

      (NOTE: Package must be signed on its face by the official who signs this letter)

   d. The point of departure is COMNAVRESFOR, Norfolk, Virginia with destination of (City, State) and return to Norfolk, Virginia. (Include known transfer points.)

   e. This authorization is effective (date) and expires (date).

      (NOTE: Not to exceed 7 days from date of issue)

Enclosure (1)
4. The Command SM for Organization, (XXX) XXX-XXXX, has been designated to confirm this authorization.

Command Security Manager
By direction

Enclosure (1)
APPENDIX Q

SAMPLE

Instructions for Couriers

1. You are designated as a command courier to transport classified material to and from Command/Organization Name in the performance of your official duties. This authorization does not include hand-carrying classified material aboard commercial aircraft. You will familiarize yourself with the following provisions:

   a. Materials transported shall remain in your physical possession at all times if proper storage at a U.S. Government activity is not available. Classified material shall not be left in such places as locked automobiles, hotel/motel rooms, safes, train compartments, public lockers, etc.; Under no circumstances will classified material (i.e. working papers, correspondence courses) be transported to your private residence.

   b. Classified material shall not be read, studied, displayed or used in any manner in public conveyances or places.

   c. When the material is carried in a private, public or government conveyance, it shall not be stowed in any detachable stowage compartment such as a trailer, luggage racks, etc.

   d. If a search of your person and belongings is required by proper authority, take these steps:

      (1) Permit search by any method that does not compromise or destroy classified material in your possession or;

      (2) If material being carried would be destroyed or compromised by the usual search methods, request appropriate inspecting official to verify your official status with this command by contacting (XXX) XXX-XXXX.

2. For military personnel, you will carry on your person DD Form 2501, Courier Authorization Card, your military identification card and the original of your travel orders (if applicable). For civilian personnel, you will carry, in addition to the DD Form 2501, your Optional Form 55 and your travel orders (if applicable).

Enclosure (1)
3. A list of classified material to be transported in possession must be provided prior to your departure from the command.

4. Card must be safeguarded at all times when not in use. I have read and understand the provisions set above.

__________________________  __________________________  _______________________
PRINT                      SIGN                               DATE

Print/Type Name Directorate

For ___________ Security Personnel to Fill in Card No#: ___________

Issue Date
APPENDIX R

COMPELLING NEED STATEMENT

LETTERHEAD

From: Commanding Officer, Navy Reserve Unit <or> Gaining Command
To: Commander, Navy Reserve Forces Command N2/Senior Intelligence Officer
Via: Supported Command Commanding Officer <or> Operational Support Officer
      NOSC <or> RCC Security Manager

Subj: COMPELLING NEED STATEMENT ICO OF [RANK/RATE, FIRST NAME, LAST NAME]

1. This letter documents a compelling need for Top Secret (TS) <or> Top Secret-Sensitive Compartmented Information (TS//SCI) access in the case of [Last Name, First Name, Middle Initial, Rank/Rate, USN, XXX-XX-last four digits of SSN].

2. [Named individual] is assigned to [billet] in [unit] and requires the access to perform duties assigned by the gaining command as described here: Justify the request in this paragraph.

3. [Gaining command] concurs with the need for access as described above.

4. This billet is not currently coded for this access. [State status of change to the billet coding, or if no plan to change the coding, explain why]. NOTE: If the billet is already coded for TS or TS/SCI access, there is no requirement for a compelling need statement.

5. My point of contact is [use military email account only; include phone number as well].

Signature

R-1 Enclosure (1)